
Mathématiques

Cours, exercices et problèmes

Terminale S

François THIRIOUX

Lycée René Perrin – Ugine – Savoie

`Francois.Thirioux@ac-grenoble.fr`

2013-2014

version du 22 juin 2013

Préambule

Pratique d'un cours photocopié

Le photocopié n'est qu'un *résumé de cours*. Il ne contient pas tous les schémas, exercices d'application, algorithmes ou compléments prodigués en classe. Il est indispensable de tenir des *notes de cours* afin de le compléter.

Compléments

Certains passages vont au-delà des objectifs *exigibles* du programme de terminale S. Le programme complet (B.O. spécial n°8 du 13/10/2011) indique clairement qu'on ne saurait se restreindre aux capacités minimales attendues.

Notations

Une expression en italique indique une définition ou un point important.

Logiciels

Une liste de logiciels libres ou de liens librement accessibles est donnée sur le blog

`www.ac-grenoble.fr/ugine/maths`

Il faudra **Geogebra** (géométrie, courbes), **LibreOffice** (tableur) et **Sage** (programmation, calcul formel). Ce dernier tourne uniquement sous Linux mais est accessible en ligne via `www.sagenb.org` ou `www.sagemath.org/eval.html` .

Devoirs à la maison

Les exercices sont de difficulté très variable et les objectifs poursuivis sont divers :

- ★ Peu difficile – à faire par tous pour la préparation du bac.
- ★★ Moyennement difficile – à considérer pour toute poursuite d'études scientifiques.
- ★★★ Très difficile – à essayer pour toute poursuite d'études exigeante en maths.

Ces étoiles sont simplement un indicateur de la difficulté globale d'un exercice : certaines questions peuvent être très simples !

Questions de cours

Les points suivants peuvent être abordés dans le cadre d'une restitution organisée de connaissances (ROC) à l'épreuve écrite du bac.

- 2 - Suites – Si (u_n) et (v_n) sont deux suites telles que $u_n \leq v_n$ à partir d'un certain rang et si $\lim u_n = +\infty$ alors $\lim v_n = +\infty$.
- 2 - Suites – Si une suite est croissante et converge vers ℓ alors tous les termes de cette suite sont $\leq \ell$.
- 2 - Suites – La suite (q^n) avec $q > 1$ tend vers $+\infty$.
- 2 - Suites – Une suite croissante et non majorée tend vers $+\infty$.
- 6 - Exponentielle – Unicité d'une fonction f dérivable sur \mathbb{R} vérifiant $f' = f$ et $f(0) = 1$.
- 6 - Exponentielle – On a $\lim_{x \rightarrow +\infty} e^x = +\infty$ et $\lim_{x \rightarrow -\infty} e^x = 0$.
- 9 - Conditionnement et indépendance – Si A et B sont deux événements indépendants alors \overline{A} et B aussi.
- 10 - Intégration – Si f est une fonction continue, positive et croissante sur $[a; b]$ alors la fonction $F : x \mapsto \int_a^x f$ est une primitive de f .
- 11 - Produit scalaire – Théorème du toit : soient deux plans sécants contenant deux droites parallèles ; alors la droite d'intersection des deux plans est parallèle aux deux droites.
- 11 - Produit scalaire – L'équation $ax + by + cz + d = 0$ (avec a, b, c non tous nuls) caractérise les points d'un plan.
- 11 - Produit scalaire – Une droite est orthogonale à toute droite d'un plan ssi elle est orthogonale à deux droites sécantes de ce plan.
- 13 - Lois de probabilité – Une v.a. T qui suit une loi exponentielle est sans vieillissement : $P_{T \geq t}(T \geq t + h) = P(T \geq h)$.
- 13 - Lois de probabilité – L'espérance d'une v.a. suivant la loi exponentielle de paramètre λ vaut $\frac{1}{\lambda}$.
- 13 - Lois de probabilité – Pour $\alpha \in]0; 1[$ et X une v.a. de loi $\mathcal{N}(0; 1)$, il existe un unique réel positif u_α vérifiant $P(-u_\alpha \leq X \leq u_\alpha) = 1 - \alpha$.
- 13 - Lois de probabilité – Si X_n est une v.a. qui suit la loi $\mathcal{B}(n, p)$ alors pour tout $\alpha \in]0; 1[$ on a $\lim_{n \rightarrow +\infty} P\left(\frac{X_n}{n} \in I_n\right) = 1 - \alpha$ où $I_n = \left[p - u_\alpha \frac{\sqrt{p(1-p)}}{\sqrt{n}}; p + u_\alpha \frac{\sqrt{p(1-p)}}{\sqrt{n}}\right]$.
- 13 - Lois de probabilité – Soit p une proportion fixée ; lorsque n est assez grand, l'intervalle $\left[\frac{X_n}{n} - \frac{1}{\sqrt{n}}; \frac{X_n}{n} + \frac{1}{\sqrt{n}}\right]$ contient la proportion p avec une probabilité d'au moins 0,95.

Table des matières

I	Cours et exercices – Tronc commun	10
1	Limites	11
1.1	Généralités	11
1.2	Opérations	12
1.3	Comparaison	14
1.4	Exercices	16
2	Suites numériques	18
2.1	Récurrence	18
2.2	Propriétés des suites réelles	19
2.3	Existence de limite	20
2.4	Exercices	23
3	Continuité	27
3.1	Généralités	27
3.2	Théorème des valeurs intermédiaires	27
3.3	Compléments	29
3.4	Exercices	31
4	Dérivation	32
4.1	Généralités	32
4.2	Opérations	33
4.3	Variations	34
4.4	Exercices	36
5	Fonctions trigonométriques	39
5.1	Cercle trigonométrique	39
5.2	Dérivabilité	39
5.3	Propriétés	41
5.4	Exercices	43
6	Exponentielle	45
6.1	Construction et propriétés élémentaires	45
6.2	Propriétés algébriques et notation exponentielle	46
6.3	Propriétés analytiques	47
6.4	Construction de l'exponentielle	48
6.5	Exercices	50

7	Nombres complexes	54
7.1	Généralités	54
7.2	Conjugué et module	54
7.3	Équations du second degré	55
7.4	Propriétés géométriques	56
7.5	Exponentielle complexe	57
7.6	Cercles et rotations	59
7.7	Exercices	60
8	Logarithme	65
8.1	Construction	65
8.2	Propriétés	65
8.3	Fonctions puissances	67
8.4	Exercices	69
9	Conditionnement et indépendance	72
9.1	Espaces probabilisés	72
9.2	Conditionnement et indépendance	73
9.3	Probabilités totales	75
9.4	Exercices	76
10	Intégration	80
10.1	Intégrale d'une fonction continue	80
10.2	Propriétés	82
10.3	Calcul d'intégrales	84
10.4	Exercices	86
11	Produit scalaire	92
11.1	Expressions du produit scalaire	92
11.2	Plans	92
11.3	Exercices	95
12	Droites et plans	97
12.1	Barycentres	97
12.2	Plans	97
12.3	Droites	98
12.4	Intersections	98
12.5	Exercices	99
13	Lois de probabilité	101
13.1	Loi binomiale	101
13.2	Densité	103
13.3	Loi uniforme	104
13.4	Loi exponentielle	105

13.5	Loi normale	105
13.6	Fluctuation et estimation	108
13.7	Exercices	111
II	Cours et exercices – Spécialité	118
1	Divisibilité	119
1.1	Divisibilité dans \mathbb{Z}	119
1.2	Division euclidienne	119
1.3	Pgcd, ppcm, algorithme d'Euclide	120
1.4	Congruences	121
1.5	Grands théorèmes	122
1.6	Exercices	124
2	Nombres premiers	128
2.1	Généralités	128
2.2	Décomposition	128
2.3	Petit théorème de Fermat	129
2.4	Exercices	130
3	Matrices	133
3.1	Généralités	133
3.2	Opérations algébriques	133
3.3	Matrices carrées	134
3.4	Exercices	136
4	Modèles matriciels	139
4.1	Chiffrement de Hill	139
4.2	Suites récurrentes matricielles linéaires	139
4.3	Suites récurrentes matricielles affines	140
4.4	Modèle d'évolution de Lotka-Volterra	140
4.5	Marches aléatoires	141
III	Devoirs à la maison – Tronc commun	147
1	Formules trigonométriques	148
1.1	Formules courantes	148
1.2	Formules de changement de variable	148
2	Relativité très restreinte	149
2.1	Cône de lumière de Minkowski	149
2.2	Produit de Lorentz	149

3	Modèle logistique discret	150
3.1	Présentation du problème	150
3.2	Étude partielle du modèle logistique	151
4	Suites et nombre d'or	152
4.1	Le nombre d'or	152
4.2	La suite (a_n)	152
4.3	Puissances du nombre d'or	153
4.4	Suite de Fibonacci	153
5	Études de suites	154
5.1	Mensualités d'un emprunt	154
5.2	Algorithme de Babylone	154
5.3	Moyenne arithmético-géométrique	155
6	Classes de fonctions continues	156
6.1	Résolution d'une équation fonctionnelle	156
6.2	Fonctions contractantes	156
6.3	Isométries de la droite réelle	157
6.4	Fonctions continues commutant	157
7	Géométrie et optimisation	158
7.1	Aire maximale	158
7.2	Distance d'un point à une parabole	158
7.3	Tangente commune	158
7.4	Photographie de la statue de la Liberté	158
8	Études de fonctions	159
8.1	Une fonction rationnelle	159
8.2	Développements limités du sinus et du cosinus	160
9	Fonctions trigonométriques	161
9.1	Fonction arctangente	161
9.2	Une somme de Fourier	162
10	Le nombre e	163
10.1	Étude de deux suites	163
10.2	Calcul exact de la limite	163
10.3	Irrationalité de e	163
11	Compléments sur l'exponentielle	164
11.1	Position par rapport aux tangentes	164
11.2	Minorations polynômiales	164
11.3	Convexité	164

12 Méthode de Newton	165
12.1 Étude générale et existence d'une racine	165
12.2 Approximation de la racine	165
13 Complexes et polynômes	166
13.1 Racines carrées d'un complexe	166
13.2 Positions des racines d'un polynôme	166
13.3 Racines d'un polynôme à coefficients réels	166
13.4 Contrôle du module d'une racine d'un polynôme	166
13.5 Théorème fondamental de l'algèbre	167
14 Complexes et électronique linéaire	168
14.1 Impédance	168
14.2 Propriétés	169
14.3 Représentation de l'impédance	169
15 Complexes et géométrie	170
15.1 Homographie et cercles	170
15.2 Suites de Mendès-France	170
16 Applications du logarithme	171
16.1 Sismologie	171
16.2 Radioactivité	171
16.3 Astronomie	172
16.4 Acoustique	172
16.5 Datation	172
17 Compléments sur le logarithme	173
17.1 Développement limité	173
17.2 Constante d'Euler	173
18 Conditionnement et indépendance	174
18.1 Surprises conditionnelles	174
18.2 Indépendances	174
18.3 Transmission d'une rumeur	174
19 Probabilités en biologie	175
19.1 Formule de Bayes	175
19.2 Théorème d'Hardy-Weinberg	175
20 Intégration et ordre	176
20.1 Suites et intégrales	176
20.2 Intégration des fonctions périodiques	176
20.3 Inégalité de Cauchy-Schwarz	176

21	Intégration et sommes	177
21.1	Centre d'inertie d'un demi-disque	177
21.2	Encadrement du logarithme népérien	177
21.3	Approximation de π par la méthode de l'arctangente	178
22	Intégrales trigonométriques	179
22.1	Intégrale de Wallis	179
22.2	Somme des inverses des carrés	180
23	Produit scalaire dans l'espace	181
23.1	Orthogonalité de deux droites	181
23.2	Propriétés du tétraèdre régulier	181
24	Systèmes linéaires	182
24.1	Calculs d'entraînement	182
24.2	Nouvelle base de l'espace des polynômes $\mathbb{R}[x]$	182
25	Géométrie analytique	183
25.1	Premier QCM	183
25.2	Second QCM	184
26	Dénombrement	185
26.1	Parties d'un ensemble	185
26.2	Problème des parties	185
26.3	Dénombrement par partitionnement	185
26.4	Formule du binôme	186
26.5	Calculs de sommes binomiales	186
26.6	Formule de Leibniz	186
27	Compléments de probabilités	187
27.1	Approximation par une loi de Poisson	187
27.2	Simulation de la loi exponentielle	187
27.3	Fonction gamma	187
27.4	Loi faible des grands nombres	188
28	Autour de la loi normale	189
28.1	Méthode de Monte-Carlo	189
28.2	Mélange de gaz	189
28.3	Test de normalité	189
IV	Devoirs à la maison – Spécialité	190
1	Méthode de Fermat	191
1.1	Introduction	191

1.2	Algorithme	191
2	Polynômes à coefficients entiers	193
2.1	Racines rationnelles	193
2.2	Applications	193
3	Nombres de Mersenne	194
3.1	Racine carrée modulaire de 2	194
3.2	Factorisation de M_q	194
3.3	Factorisation de M_{11}	194
3.4	Pgcd de deux nombres de Mersenne	195
4	Nombres de Fermat	196
4.1	Racine carrée modulaire de 2	196
4.2	Origine des nombres de Fermat	196
4.3	Primalité des nombres de Fermat	196
4.4	Pgcd de deux nombres de Fermat	196
5	Formes de nombres premiers	197
5.1	La forme $4n + 1$	197
5.2	La forme $6n + 1$	197
6	Ordre	198
6.1	Ordre modulo p	198
6.2	Théorème de Wilson	198
7	Nombres de Carmichael et critère de Korselt	199
7.1	Introduction	199
7.2	Preuve du théorème de Korselt	200
8	Coût de l'algorithme d'Euclide	201
9	Fonction indicatrice d'Euler	202

Partie I

Cours et exercices – Tronc commun

1. Limites

1.1 Généralités

1.1.1 Limite en $\pm\infty$

Définition. • Soit $\ell \in \mathbb{R}$. Une fonction f *converge* (ou *tend*) vers ℓ en $+\infty$ si tout intervalle ouvert contenant ℓ contient toutes les valeurs de $f(x)$ pour x assez grand. On note alors $\lim_{x \rightarrow +\infty} f(x) = \ell$ ou $\lim_{+\infty} f = \ell$.

- Une fonction f *diverge* (ou *tend*) vers $+\infty$ en $+\infty$ si $f(x)$ dépasse n'importe quel réel A pour x assez grand. On note alors $\lim_{x \rightarrow +\infty} f(x) = +\infty$ ou $\lim_{+\infty} f = +\infty$.

Remarque. Les définitions sont évidemment analogues avec $-\infty$.

Théorème (fonctions de référence). Les fonctions \sqrt{x} et x^n ($n \in \mathbb{N}^*$) tendent vers $+\infty$ lorsque x tend vers $+\infty$.

Preuve. On démontre par exemple que x^2 tend vers $+\infty$ en $+\infty$. Soit A un réel positif quelconque. Si $x > \sqrt{A}$ alors $x^2 > A$. Par définition, on a le résultat souhaité. \square

1.1.2 Limite en un réel

Définition. • Soit $a \in \mathbb{R}$. Une fonction f *diverge* (ou *tend*) vers $+\infty$ en a si $f(x)$ dépasse n'importe quel réel A pour x assez voisin de a . On note alors $\lim_{x \rightarrow a} f(x) = +\infty$ ou $\lim_a f = +\infty$.

- Soient $a \in \mathbb{R}$ et $\ell \in \mathbb{R}$. Une fonction f *converge* (ou *tend*) vers ℓ en a si tout intervalle ouvert contenant ℓ contient toutes les valeurs de $f(x)$ pour x assez voisin de a . On note alors $\lim_{x \rightarrow a} f(x) = \ell$ ou $\lim_a f = \ell$.

Remarque. Le premier point de la définition s'étend évidemment avec $-\infty$.

Théorème. Si une fonction f est définie en a et y admet une limite finie ℓ , alors $\ell = f(a)$.

Preuve (idée). On montre facilement que $f(a)$ appartient à tout intervalle I contenant ℓ . Si $f(a) \neq \ell$, c'est impossible. \square

1.1.3 De l'usage des ε

Lorsque l'on veut prouver qu'une fonction f possède une limite finie ℓ en $a \in \mathbb{R} \cup \{\pm\infty\}$, on est concrètement amené à considérer que l'intervalle ouvert autour de ℓ est de la forme $]\ell - \varepsilon; \ell + \varepsilon[$. On peut montrer que $f(x)$ tend vers ℓ en prouvant que $|f(x) - \ell|$ tend vers 0 :

- choisir un réel $\varepsilon > 0$ quelconque ;
- montrer que si x est suffisamment proche de a , alors $|f(x) - \ell| < \varepsilon$.

1.1.4 Limites à gauche et à droite

Parfois une fonction ne possède pas de limite, mais possède une limite à gauche ou à droite (penser par exemple à la fonction inverse en 0).

Définition. • Soit $a \in \mathbb{R}$. Une fonction f *diverge* (ou *tend*) vers $+\infty$ à *gauche* de a si $f(x)$ dépasse n'importe quel réel A pour x assez voisin de a et $x < a$. On note alors $\lim_{\substack{x \rightarrow a \\ x < a}} f(x) = +\infty$ ou $\lim_{x \rightarrow a^-} f(x) = +\infty$ ou $\lim_{a^-} f = +\infty$.

• Soient $a \in \mathbb{R}$ et $\ell \in \mathbb{R}$. Une fonction f *converge* (ou *tend*) vers ℓ à *gauche* de a si tout intervalle ouvert contenant ℓ contient toutes les valeurs de $f(x)$ pour x assez voisin de a et $x < a$. On note alors $\lim_{\substack{x \rightarrow a \\ x < a}} f(x) = \ell$ ou $\lim_{x \rightarrow a^-} f(x) = \ell$ ou $\lim_{a^-} f = \ell$.

Remarque. • Les définitions sont évidemment analogues à *droite*, et on note alors $x \rightarrow a^+$.

• Lorsqu'une quantité conserve (par exemple) un signe positif, on peut l'affubler d'un exposant $+$ qui peut être utile. Par exemple, comme on le verra par la suite, $\lim_{x \rightarrow 0} \frac{1}{x^2}$ est de la forme « $\frac{1}{0^+}$ » et vaut donc $+\infty$, alors que simplement « $\frac{1}{0}$ » est une forme indéterminée.

Théorème. Soit f une fonction définie (sauf éventuellement en a) sur un intervalle contenant a . La fonction f possède une limite en a si et seulement si f possède des limites à gauche et à droite égales (à $f(a)$ si f est définie en a).

Preuve. Il suffit de revenir aux définitions. □

1.1.5 Unicité de la limite

Les fonctions ne possèdent pas le don d'ubiquité :

Théorème (unicité de la limite). Si une fonction converge alors sa limite est unique.

Preuve. Plaçons-nous par exemple en $+\infty$. Soit f une fonction définie au voisinage de $+\infty$, et supposons qu'elle possède deux limites distinctes ℓ et ℓ' . Il existe un réel A tel que $x > A$ implique $|f(x) - \ell| < \frac{|\ell - \ell'|}{2}$. De même, il existe un réel A' tel que $x > A'$ implique $|f(x) - \ell'| < \frac{|\ell - \ell'|}{2}$. Ainsi, si $x > \max(A, A')$, $|\ell - \ell'| \leq |\ell - f(x)| + |f(x) - \ell'| < \frac{|\ell - \ell'|}{2} + \frac{|\ell - \ell'|}{2} = |\ell - \ell'|$. Absurde. □

1.2 Opérations

En pratique, on calcule souvent une limite en combinant les résultats préétablis sur les fonctions de référence et non pas en revenant à chaque fois à la définition. Nous allons seulement prouver les résultats les plus importants.

Soient f et g deux fonctions ayant pour limites ℓ et ℓ' en un réel a ou en $a = \pm\infty$.

1.2.1 Somme

Théorème. $\lim_a f + g = \ell + \ell'$.

Preuve. Supposons ici que $a = +\infty$ (le cas $a \in \mathbb{R}$ se traite identiquement). Soit $\varepsilon > 0$. Il existe un réel A tel que $x > A$ implique $|f(x) - \ell| < \frac{\varepsilon}{2}$ et un réel A' tel que $x > A'$ implique $|g(x) - \ell'| < \frac{\varepsilon}{2}$. Si $x > \max(A, A')$ alors $|(f + g)(x) - (\ell + \ell')| = |(f(x) - \ell) + (g(x) - \ell')| < |f(x) - \ell| + |g(x) - \ell'| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$. Par définition, $\lim_{x \rightarrow \infty} f + g = \ell + \ell'$. \square

1.2.2 Produit

Lemme. Si $\ell = 0$ alors $\lim_a fg = 0$.

Preuve. Supposons ici que $a = +\infty$ (le cas $a \in \mathbb{R}$ se traite identiquement). Soit $\varepsilon > 0$. Il existe un réel A tel que $x > A$ implique $|f(x)| < \varepsilon$ et un réel A' tel que $x > A'$ implique $|g(x) - \ell'| < \varepsilon$. Si $x > \max(A, A')$ alors $|f(x)g(x)| = |f(x)(g(x) - \ell') + f(x)\ell'| \leq |f(x)||g(x) - \ell'| + |f(x)||\ell'| < \varepsilon^2 + |\ell'|\varepsilon$. Cette dernière expression tend bien vers 0 lorsque ε tend vers 0. \square

Théorème. $\lim_a fg = \ell\ell'$.

Preuve. On forme $f(x)g(x) - \ell\ell' = \underbrace{g(x)}_{\rightarrow \ell'} \underbrace{(f(x) - \ell)}_{\rightarrow 0} + \underbrace{\ell}_{\text{cste}} \underbrace{(g(x) - \ell')}_{\rightarrow 0}$, expression qui tend bien vers 0 d'après le lemme. \square

1.2.3 Quotient

Théorème. $\lim_a \frac{f}{g} = \frac{\ell}{\ell'}$ si $\ell' \neq 0$.

Preuve. Admise. \square

1.2.4 Composée

Théorème. Soient $a, b, \ell \in \mathbb{R} \cup \{\pm\infty\}$. Si $\lim_{x \rightarrow a} f(x) = b$ et $\lim_{y \rightarrow b} g(y) = \ell$ alors $\lim_{x \rightarrow a} g(f(x)) = \ell$.

Preuve (idée). Si y est suffisamment proche de b , alors $g(y)$ devient voisin de $g(b)$. Pour rendre y suffisamment proche de b , il suffit de rendre x suffisamment voisin de a . \square

1.2.5 Formes indéterminées

Si beaucoup d'opérations ont un résultat facile à mémoriser (par exemple « $(-2) \times (+\infty) = -\infty$ »), certaines ne conduisent pas à un résultat systématique. Ce sont les *formes indéterminées* : $(+\infty) - (+\infty)$, $(+\infty) \times 0$, $\frac{+\infty}{+\infty}$, $\frac{?}{0}$. Dans ces situations, il existe des techniques pour lever l'indétermination (cf exercices).

1.2.6 Polynômes et fractions rationnelles

Théorème. La limite d'un polynôme en $\pm\infty$ est donnée par celle de son terme de plus haut degré.

Preuve. Soit $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$. On factorise par le terme dominant en $\pm\infty$, à savoir $a_n x^n$: $P(x) = a_n x^n (1 + \frac{a_{n-1}}{a_n} x^{-1} + \dots + \frac{a_1}{a_n} x^{-(n-1)} + \frac{a_0}{a_n} x^{-n})$. Il est facile de montrer que la parenthèse tend vers 1, d'où le résultat. \square

Théorème. La limite d'une fraction rationnelle en $\pm\infty$ est donnée par celle du quotient des termes de plus hauts degrés de son numérateur et de son dénominateur.

Preuve. La méthode est identique à celle de la preuve précédente. \square

Exemple. Soit $f(x) = \frac{2x^2 + 3}{x^4 + x^2 + 1}$. On peut écrire directement $\lim_{x \rightarrow +\infty} f(x) = \lim_{x \rightarrow +\infty} \frac{2x^2}{x^4} = \lim_{x \rightarrow +\infty} \frac{2}{x^2} = 0$.

1.3 Comparaison

1.3.1 Inégalités

Théorème. Soit $a \in \mathbb{R} \cup \{\pm\infty\}$.

- (encadrement) Si, pour x voisin de a , on a $g(x) \leq f(x) \leq h(x)$ et si g et h ont la même limite finie ℓ en a , alors f converge en a vers ℓ .
- (minoration) Si, pour x voisin de a , on a $g(x) \leq f(x)$ et si $\lim_{x \rightarrow a} g(x) = +\infty$, alors f diverge en a vers $+\infty$.
- (majoration) Si, pour x voisin de a , on a $f(x) \leq h(x)$ et si $\lim_{x \rightarrow a} h(x) = -\infty$, alors f diverge en a vers $-\infty$.

Preuve. Démontrons le premier point pour $a = +\infty$. Soit I un intervalle ouvert contenant ℓ . Les fonctions g et h convergent vers ℓ ; il existe donc un réel G tel que $x > G$ implique $g(x) \in I$ et un réel H tel que $x > H$ implique $h(x) \in I$. Ainsi, si $x > \max(G, H)$ alors $g(x) \in I$ et $h(x) \in I$. Puisque $g(x) \leq f(x) \leq h(x)$, $f(x) \in I$ aussi. Par définition, f tend vers ℓ en a . \square

1.3.2 Asymptotes

Définition. Deux fonctions sont dites *asymptotes* en a si leur différence tend vers 0 en a .

Remarque. Ceci signifie concrètement que leurs courbes se rapprochent infiniment au voisinage de $x = a$. Deux courbes sont *asymptotes* si leurs fonctions associées le sont.

Définition.

- Si une fonction f possède une limite finie ℓ en $\pm\infty$, alors la droite d'équation $y = \ell$ est l'*asymptote horizontale* à la courbe \mathcal{C}_f en $\pm\infty$.
- Si une fonction f possède une limite infinie en $a \in \mathbb{R}$, alors la droite d'équation $x = a$ est l'*asymptote verticale* à la courbe \mathcal{C}_f en a .

- S'il existe une droite Δ d'équation $y = ax + b$ avec $a \neq 0$ asymptote à \mathcal{C}_f en $\pm\infty$, alors Δ est l'*asymptote oblique* à \mathcal{C}_f en $\pm\infty$.

Remarque. Supposons que \mathcal{C}_f possède une asymptote oblique d'équation $y = ax + b$ en $+\infty$. On a ainsi $\lim_{x \rightarrow +\infty} f(x) - (ax + b) = 0$. Par conséquent $\lim_{x \rightarrow +\infty} \frac{f(x)}{x} = a$. En pratique, on recherche donc une *éventuelle* asymptote oblique en étudiant la limite de $\frac{f(x)}{x}$, qui donne le candidat pour la pente a .

1.4 Exercices

Ce qui concerne les limites de suites (qui ne sont que des fonctions de \mathbb{N} dans \mathbb{R}) est traité dans les exercices du chapitre 2. De la même manière, certains exercices sur les limites seront traités dans le cadre des suites ou de la trigonométrie.

Généralités

1.1. Supposons qu'on ait trois fonctions définies sur \mathbb{R} et vérifiant $g(x) \leq f(x) \leq h(x)$. Peut-on affirmer que si $\lim_{x \rightarrow +\infty} g(x) = 3$ et $\lim_{x \rightarrow +\infty} h(x) = 5$ alors $3 \leq \lim_{x \rightarrow +\infty} f(x) \leq 5$?

Opérations

1.2. Calculer la limite de $\sqrt{1 + \frac{1}{x^2}}$ lorsque x tend vers $+\infty$.

1.3. Calculer la limite de $\frac{x^2 - x + 2}{(x - 2)^2}$ lorsque x tend vers 2.

1.4. Calculer la limite de $\frac{x^2 - 2x + 1}{x^2 - 3x + 2}$ lorsque x tend vers 1.

1.5. Calculer la limite de $\frac{2x^3 + 5x^2 - 3}{(x - 2)^3(1 - x)}$ lorsque x tend vers 2.

1.6. Calculer la limite de $\frac{1}{x^2 - 4}$ lorsque x tend vers 2.

Factorisation par le terme dominant

1.7. Calculer la limite de $x - \sqrt{x}$ lorsque x tend vers $+\infty$.

1.8. Calculer la limite de $x^3 - 6x + 5$ lorsque x tend vers $+\infty$.

1.9. Calculer la limite de $\frac{x^2 - 3x + 2}{x^2 + x + 2}$ lorsque x tend vers $+\infty$.

1.10. Calculer la limite de $\frac{x - \sqrt{x}}{x + 3}$ lorsque x tend vers $+\infty$.

Quantité conjuguée et taux de variation

1.11. Déterminer (par limite d'un taux d'accroissement) la dérivée de la fonction racine carrée.

1.12. Calculer la limite de $\sqrt{x+1} - \sqrt{x}$ lorsque x tend vers $+\infty$.

1.13. Calculer la limite de $\frac{2 - \sqrt{x+1}}{x - 3}$ lorsque x tend vers 3.

1.14. Calculer la limite de $\frac{\sqrt{2x+3} - \sqrt{x+4}}{x - 1}$ lorsque x tend vers 1.

Encadrement et méthodes diverses

1.15. Calculer la limite de $\frac{\lfloor x \rfloor}{x}$ lorsque x tend vers $+\infty$.

1.16. Calculer la limite de $\sqrt{x}(\sqrt{x+1} - \sqrt{x})$ lorsque x tend vers $+\infty$.

Asymptotes

1.17. Déterminer les asymptotes de la fonction f définie sur $\mathbb{R} - \{3\}$ par $f(x) = \frac{1}{(x-3)^2}$.

1.18. Soit f la fonction définie sur \mathbb{R}_+ par $f(x) = \frac{8x^2 - 4x + 1}{2x + 1}$.

1. Montrer qu'il existe des réels a , b et c tels que $f(x) = ax + b + \frac{c}{2x + 1}$.
2. En déduire que \mathcal{C}_f admet une asymptote oblique en $+\infty$.
3. Étudier leurs positions relatives.

1.19. Soit f la fonction définie sur \mathbb{R} par $f(x) = \frac{x^3 + x^2 + 3x - 2}{x^2 + 1}$.

1. Montrer qu'il existe des réels a , b , c et d tels que $f(x) = ax + b + \frac{cx + d}{x^2 + 1}$.
2. En déduire que \mathcal{C}_f admet une asymptote oblique en $\pm\infty$.
3. Étudier leurs positions relatives.

1.20. Soit f la fonction définie sur \mathbb{R} par $f(x) = \sqrt{x^2 + x}$.

Montrer que \mathcal{C}_f possède une asymptote en $+\infty$ et donner son équation.

1.21. Soit f la fonction définie sur \mathbb{R}_+ par $f(x) = \frac{x^3 - 1}{x + 1}$.

1. La fonction f possède-t-elle une asymptote en $+\infty$?
2. Montrer qu'il existe des réels a , b , c et d tels que $f(x) = ax^2 + bx + c + \frac{d}{x + 1}$.
3. En déduire une fonction polynômiale asymptote à f en $+\infty$.

1.22. Soit f une fonction *homographique*, définie sur $\mathbb{R} - \left\{-\frac{d}{c}\right\}$ par $f(x) = \frac{ax + b}{cx + d}$ avec $ad - bc \neq 0$ (ce qui exclut les cas où f est constante).

1. Montrer que \mathcal{C}_f possède une asymptote horizontale et une autre verticale.
2. Montrer que leur point d'intersection est centre de symétrie de la courbe de f .

1.23. Deux fonctions f et g sont *équivalentes* au voisinage de $a \in \mathbb{R} \cup \{\pm\infty\}$ si $\lim_{x \rightarrow a} \frac{f(x)}{g(x)} = 1$.

1. Déterminer si les fonctions $f(x) = x + \sqrt{x}$ et $g(x) = x - 3$ sont équivalentes ou asymptotes en $+\infty$.
2. Supposons $\lim_{x \rightarrow a} g(x) = +\infty$ (*par exemple*). Montrer que si f et g sont asymptotes en a , alors elles y sont équivalentes. La réciproque est-elle vraie?

2. Suites numériques

2.1 Récurrence

2.1.1 Démonstration par récurrence

Théorème (de récurrence). Soit $n_0 \in \mathbb{N}$. Soit P_n une proposition avec $n \in \mathbb{N}$ et $n \geq n_0$. Supposons que :

- (*initialisation*) P_{n_0} est vraie ;
- (*hérédité*) pour $n \geq n_0$ fixé, $P_n \Rightarrow P_{n+1}$.

Alors P_n est vraie pour tout entier $n \geq n_0$.

Preuve. Raisonnons par l'absurde. Supposons qu'il existe des entiers $n > n_0$ pour lesquels P_n soit fausse. Notons n_1 le plus petit d'entre eux. Par définition de n_1 , P_{n_1-1} est vraie. Par hérédité, P_{n_1-1+1} i.e. P_{n_1} est donc vraie, ce qui est absurde. \square

2.1.2 Exemples instructifs

Exemple. Prouver que $1 + 2 + \dots + n = \frac{n(n+1)}{2}$.

Remarque. Le raisonnement par récurrence est puissant mais ne donne pas miraculeusement la propriété à démontrer.

Exemple. Prouvons que 6 divise $7^n + 1$. Supposons P_n . Alors il existe k tel que $7^n + 1 = 6k$. Ainsi, $7^{n+1} + 1 = 7 \cdot 7^n + 1 = 7(6k - 1) + 1 = 42k - 6 = 6(7k - 1)$. Par conséquent 6 divise $7^{n+1} + 1$, i.e. P_{n+1} est vraie. Par récurrence, P_n est vraie pour tout n . Trouver l'erreur !

Remarque. Une proposition peut être héréditaire sans être pour autant vraie. Il faut toujours penser à vérifier l'initialisation.

Exemple. Prouvons que tout le monde a la même taille. On pose $P_n = \ll n \text{ personnes ont toujours la même taille} \gg$. Cette fois on n'oublie pas d'initialiser : une personne a la même taille qu'elle-même, donc P_1 est vraie. L'hérédité ensuite. Soit $n \geq 1$ et supposons que P_n est vraie. On considère donc $n + 1$ personnes. Les personnes n°1 jusqu'à n ont la même taille, par hypothèse de récurrence. De même, les personnes n°2 jusqu'à $n + 1$ ont la même taille. Ainsi, ces $n + 1$ personnes ont la même taille. Trouver l'erreur !

Remarque. L'hérédité doit être valable pour tous les rangs $\geq n_0$ sans exception.

Exemple. Prouver par récurrence puis directement que 3 divise $n^3 - n$.

Remarque. La récurrence n'est pas toujours la méthode de démonstration la plus pertinente.

2.2 Propriétés des suites réelles

2.2.1 Variations

Définition. Une suite réelle est (resp. strictement) *monotone* si elle est (resp. strictement) croissante ou (resp. strictement) décroissante.

Rappel. Pour étudier les variations d'une suite, on est souvent amené à étudier $u_{n+1} - u_n$ ou parfois $\frac{u_{n+1}}{u_n}$.

2.2.2 Frontières

Définition. Une suite réelle (u_n) est :

- *majorée* s'il existe un réel M tel que $\forall n \in \mathbb{N}, u_n \leq M$;
- *minorée* s'il existe un réel m tel que $\forall n \in \mathbb{N}, m \leq u_n$;
- *bornée* si elle est minorée et majorée.

2.2.3 Limites

Voir globalement le chapitre 1, une suite n'étant qu'une fonction de \mathbb{N} dans \mathbb{R} . Notons tout de même que la seule limite intéressante pour une suite est en $+\infty$ en raison du caractère discret de \mathbb{N} . On pourra donc omettre le « $n \rightarrow +\infty$ » sous une limite de suite.

Définition. Une suite réelle (u_n) *converge* vers un réel ℓ si tout intervalle ouvert contenant ℓ contient tous les u_n à partir d'un certain rang.

Théorème. Soient f une fonction continue (*voir le chapitre 3*) et (u_n) une suite définie par la relation de récurrence $u_{n+1} = f(u_n)$.

Si la suite (u_n) converge vers un réel ℓ , alors $\ell = f(\ell)$ i.e. ℓ est un *point fixe* de f .

Preuve. Si $\lim_{n \rightarrow +\infty} u_n = \ell$, alors par continuité de f , $\lim_{n \rightarrow +\infty} f(u_n) = f(\ell)$. De plus $\lim_{n \rightarrow +\infty} u_{n+1} = \ell$ aussi. □

Remarque. Lors d'une étude graphique de suite récurrente $u_{n+1} = f(u_n)$, on est amené à tracer la courbe \mathcal{C}_f de f ainsi que la droite d'équation $y = x$. La première bissectrice sert non seulement à construire l'évolution de la suite, mais aussi à observer les points fixes de f , qui sont les abscisses de ses intersections avec \mathcal{C}_f . Le théorème précédent montre que les points fixes de f sont les seuls candidats pour la limite de (u_n) .

Théorème. Soient f une fonction définie sur un intervalle I et (u_n) une suite à valeurs dans I . Soient $a, \ell \in \mathbb{R} \cup \{\pm\infty\}$.

Si $\lim_{n \rightarrow +\infty} u_n = a$ et $\lim_{x \rightarrow a} f(x) = \ell$ alors $\lim_{n \rightarrow +\infty} f(u_n) = \ell$.

Preuve. C'est un simple avatar du théorème de composition des limites. □

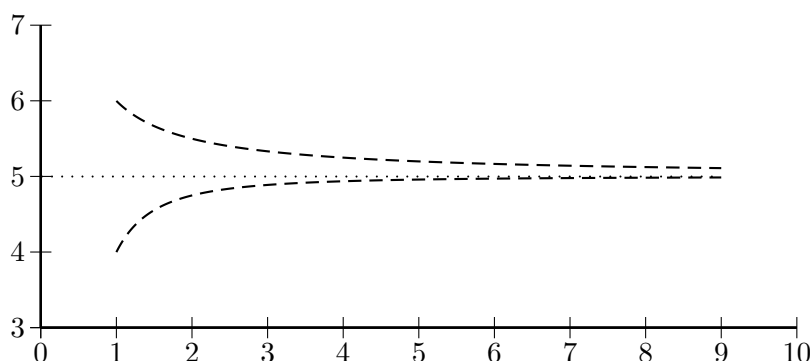
2.2.4 Suites adjacentes

Définition. Deux suites réelles (u_n) et (v_n) sont *adjacentes* si :

- (u_n) est croissante ;
- (v_n) est décroissante ;
- $u_n \leq v_n$;
- $\lim_{n \rightarrow +\infty} v_n - u_n = 0$.

Remarque. L'hypothèse $u_n \leq v_n$ n'est pas nécessaire, les trois autres l'impliquent. Elle permet cependant de mieux appréhender la notion.

Exemple. Soient $u_n = 5 + \frac{1}{n}$ et $v_n = 5 - \frac{1}{n^2}$. On commence par représenter ces suites :



On voit se dessiner l'entonnoir typique des suites adjacentes. On vérifie simplement que (u_n) est décroissante, que (v_n) est croissante et que $u_n - v_n$ tend vers 0.

2.3 Existence de limite

2.3.1 Comparaison

Reprenons le chapitre 1 dans le cas particulier des suites :

Théorème. Soient (u_n) et (v_n) deux suites vérifiant :

- $u_n \leq v_n$ à partir d'un certain rang ;
- $\lim_{n \rightarrow +\infty} u_n = +\infty$.

Alors la suite (v_n) tend également vers $+\infty$.

Preuve. Soit A un réel quelconque. Puisque (u_n) tend vers $+\infty$, il existe par définition un rang n_0 tel que si $n \geq n_0$ alors $u_n > A$. Il existe par ailleurs un rang n_1 tel que si $n \geq n_1$ alors $u_n \leq v_n$. En posant $N = \max(n_0, n_1)$, on est assuré que si $n \geq N$ alors $v_n \geq u_n > A$, ce qui prouve par définition la limite infinie de (v_n) . \square

2.3.2 Suites géométriques

Remarque. Soit $x > 0$. On a apparemment $(1+x)^n = (1+x)(1+x) \cdots (1+x) = 1 + nx + \cdots$. Les termes non écrits sont positifs et donc il semble que $(1+x)^n \geq 1 + nx$.

Lemme (inégalité de Bernoulli). Si $x > 0$ alors $(1+x)^n \geq 1+nx$ quel que soit $n \in \mathbb{N}$.

Preuve. L'inégalité est trivialement vraie pour $n = 0$. Soit $n \in \mathbb{N}$ et supposons $(1+x)^n \geq 1+nx$. On a $(1+x)^{n+1} = (1+x)^n(1+x) \geq (1+nx)(1+x) = 1+nx+x+nx^2 = 1+(n+1)x+nx^2 \geq 1+(n+1)x$. Par récurrence, le lemme est vérifié. \square

Théorème. Le comportement asymptotique de la suite géométrique (q^n) est déterminé par la valeur de sa raison q :

- si $q > 1$ alors $\lim_{n \rightarrow +\infty} q^n = +\infty$;
- si $-1 < q < 1$ alors $\lim_{n \rightarrow +\infty} q^n = 0$.

Preuve. • Si $q > 1$ alors $q = 1+x$ avec $x > 0$. Le lemme de Bernoulli montre que $q^n = (1+x)^n \geq 1+nx$; or $\lim_{n \rightarrow +\infty} 1+nx = +\infty$ (suite arithmétique). Le théorème de comparaison du paragraphe précédent prouve alors $\lim_{n \rightarrow +\infty} q^n = +\infty$.

- Si $-1 < q < 1$ et $q \neq 0$ alors notons $q' = \frac{1}{|q|}$. On a $q' > 1$ donc $\lim_{n \rightarrow +\infty} q'^n = +\infty$ et ainsi $\lim_{n \rightarrow +\infty} |q|^n = \lim_{n \rightarrow +\infty} \frac{1}{q'^n} = 0$. Remarquons ensuite que $-|q|^n \leq q^n \leq |q|^n$; le théorème d'encadrement montre la convergence de q^n vers 0.

\square

2.3.3 Suites monotones

Lorsqu'on se donne une suite et qu'on veut déterminer sa limite éventuelle, le problème qui se pose est qu'on ne peut pas travailler avec cette limite tant qu'on ne sait pas qu'elle existe ! Dans cette section, nous allons énoncer des théorèmes d'existence (*et non de calcul*) de limite.

Théorème (des suites adjacentes). Soient (u_n) et (v_n) deux suites adjacentes, avec $u_n \leq v_n$. Alors ces deux suites :

- convergent...
- vers la même limite ℓ ...
- qui est l'unique réel vérifiant $u_n \leq \ell \leq v_n$ pour tout n .

Preuve. Admise, elle découle de la construction de \mathbb{R} , qui est hors de portée. \square

Le théorème suivant est fondamental, il nous servira dans plusieurs situations. Son principe est déjà connu, mais sa preuve reste à établir.

Théorème (de dichotomie). Soit R un critère de choix. Soit $(I_n) = ([a_n; b_n])$ une suite d'intervalles engendrés par dichotomie sur le critère R :

- $I_0 = [a_0; b_0]$;
- en posant $c_n = \frac{a_n + b_n}{2}$ le milieu de I_n , $I_{n+1} = [a_n; c_n]$ ou $I_{n+1} = [c_n; b_n]$ suivant le critère R .

Alors la suite (I_n) converge vers un réel ℓ (i.e. (a_n) et (b_n) convergent vers la même limite ℓ).

Preuve. Par construction :

- (a_n) est croissante ;
- (b_n) est décroissante ;
- $b_n - a_n = \frac{b_0 - a_0}{2^n} \rightarrow 0$.

Ainsi (a_n) et (b_n) sont adjacentes et donc convergent vers un même réel ℓ . \square

Théorème (de convergence monotone). On a les deux résultats suivants :

- si une suite est croissante et majorée alors elle converge ;
- si une suite est décroissante et minorée alors elle converge.

Preuve. Le deuxième point est clairement équivalent au premier, en considérant l'opposé de la suite. On va ici montrer un résultat plus fort que nécessaire, à savoir l'équivalence des théorèmes des suites adjacentes et de convergence monotone.

- $TCM \Rightarrow TSA$. Soient (u_n) et (v_n) deux suites adjacentes, avec $u_n \leq v_n$. La suite (u_n) est croissante et majorée par v_0 , donc elle converge vers un réel ℓ . La suite (v_n) est décroissante et minorée par u_0 , donc elle converge vers un réel ℓ' .

On en déduit $\lim_{n \rightarrow +\infty} u_n - v_n = \lim_{n \rightarrow +\infty} u_n - \lim_{n \rightarrow +\infty} v_n = \ell - \ell'$. Ainsi $\ell - \ell' = 0$ i.e. $\ell = \ell'$.

Ensuite, quels que soient p et q , $u_p \leq v_q$. En faisant tendre p vers $+\infty$, on obtient $\ell \leq v_q$ quel que soit q . De même, $u_p \leq \ell$ quel que soit p . Il suit $u_n \leq \ell \leq v_n$ quel que soit n .

- $TSA \Rightarrow TCM$. Soit (u_n) une suite croissante et majorée par un réel M . Soit $I_0 = [u_0; M]$; cet intervalle contient nécessairement tous les u_n . Soient $I'_1 = \left[u_0; \frac{u_0 + M}{2} \right]$ et $I''_1 = \left[\frac{u_0 + M}{2}; M \right]$. Si l'on a un terme de la suite (u_n) dans I''_1 , alors ils y sont tous à partir d'un certain rang puisque la suite (u_n) est croissante et majorée par M . On choisit alors $I_1 = I''_1$. Dans le cas contraire, c'est I'_1 qui contient tous les termes de la suite (u_n) à partir d'un certain rang, et on choisit alors $I_1 = I'_1$. On définit ainsi une dichotomie de I_0 .

Chaque I_n ainsi construit contient tous les termes de la suite à partir d'un certain rang. Or, (I_n) converge vers un certain réel ℓ d'après le théorème de dichotomie.

Soit J l'intervalle $]\ell - \varepsilon; \ell + \varepsilon[$. Pour n assez grand, $I_n \subset J$, donc tous les u_n à partir d'un certain rang appartiennent à J . Par définition, la suite (u_n) converge vers ℓ . \square

Remarque. Une suite croissante et majorée par M converge, certes, mais pas nécessairement vers M . Par exemple, la suite de terme général $3 - \frac{1}{n}$ est majorée par π mais converge vers 3.

Théorème (des suites monotones). Une suite monotone et non bornée diverge vers $\pm\infty$:

- si une suite est croissante et non majorée alors elle diverge vers $+\infty$;
- si une suite est décroissante et non minorée alors elle diverge vers $-\infty$.

Preuve. Les deux assertions sont clairement équivalentes ; démontrons la première.

Soit (u_n) une suite croissante et non majorée. Soit α un réel quelconque. Il existe un rang n_0 tel que $u_{n_0} > \alpha$ puisque (u_n) n'est pas majorée (on aurait sinon $u_n \leq \alpha$ pour tout n). La suite (u_n) est croissante, donc $u_{n_0+1}, u_{n_0+2}, \dots$ sont aussi $> \alpha$. On vient ainsi de montrer $\forall \alpha \in \mathbb{R}, \exists n_0 \in \mathbb{N}, n \geq n_0 \Rightarrow u_n \geq \alpha$, ce qui est la définition de $u_n \rightarrow +\infty$. \square

Corollaire. Une suite monotone converge vers un réel ou diverge vers $\pm\infty$.

2.4 Exercices

Généralités

2.1. Montrer que si une suite est croissante et converge vers ℓ alors tous ses termes sont inférieurs ou égaux à ℓ .

2.2. Montrer que si une suite converge vers un réel ℓ non nul, alors elle est du signe de ℓ à partir d'un certain rang.

2.3. Montrer qu'une suite convergente est bornée.

2.4. 1. Montrer que si (u_n) converge alors $\lim_{n \rightarrow +\infty} u_{n+1} - u_n = 0$.

2. Montrer que la réciproque est fausse.

Interpréter $u_{n+1} - u_n$ comme un taux d'accroissement afin de trouver un contre-exemple.

2.5. Soit (u_n) la suite définie par ses deux premiers termes u_0 et u_1 , et la relation de récurrence $u_{n+2} = u_{n+1} - u_n$. Montrer que (u_n) est périodique.

2.6. Soit (u_n) la suite définie par $u_0 = 1$ et $u_{n+1} = u_n + \frac{1}{u_n}$. On admet que $u_n > 0$ quel que soit n . Montrer que (u_n) est croissante puis déterminer sa limite.

Bases sur les suites arithmétiques et géométriques

2.7. Déterminer la suite arithmétique (u_n) sachant que $u_3 = 5$ et $u_5 = 3$.

2.8. Calculer la somme des 500 premiers termes de la suite arithmétique de premier terme -5 et de raison 10.

2.9. Déterminer la suite géométrique (u_n) sachant que $u_5 = 100$ et $u_8 = 12,5$.

2.10. Calculer $2^3 + 2^4 + \dots + 2^{1789}$.

Suites géométriques

2.11. On observe une tumeur : certaines cellules sont saines mais d'autres sont malades. Un traitement permet de transformer chaque jour une certaine proportion p des cellules malades en cellules saines. Malheureusement, une certaine proportion q des cellules malades devient résistante au traitement. Une proportion r des cellules malades n'est pas touchée par le traitement, et reste malade.

On va étudier, en fonction du nombre n de jours de traitement, l'évolution des proportions de cellules saines (a_n) , malades (b_n) et malades résistantes (c_n) .

On pose par exemple $a_0 = 0,99$, $b_0 = 0,009$ et $c_0 = 0,001$.

1. Que vaut $p + q + r$? $a_n + b_n + c_n$?

2. On suppose dans la suite que $p = 0,1$ et $q = 0,01$.

- (a) Exprimer a_{n+1} , b_{n+1} et c_{n+1} en fonction de a_n , b_n et c_n .
 - (b) Observer l'évolution (*variations, limites, vitesse de convergence...*) des trois suites grâce à un tableur.
 - (c) Montrer que (b_n) est géométrique.
 - (d) En déduire son terme général puis ceux de (a_n) et (c_n) .
 - (e) Déterminer les limites de ces trois suites.
 - (f) Vérifier ces résultats sur la feuille de calcul du tableur.
3. Combien de jours sont nécessaires à une stabilisation de la proportion de cellules saines au millièème près ?
4. Que peut-on conclure sur l'efficacité du traitement (*points positifs et négatifs*) ?

2.12. Soit (u_n) la suite (*arithmético-géométrique ou récurrente affine*) définie par u_0 et $u_{n+1} = au_n + b$ avec $a \neq 1$ (*évite les suites arithmétiques*) et $b \neq 0$ (*évite les suites géométriques*).

- 1. Si (u_n) converge, que vaut sa limite ℓ ?
- 2. Montrer que $(u_n - \ell)$ est géométrique.

On vient en fait d'effectuer un changement de repère pertinent.

2.13. Étudier graphiquement puis rigoureusement la convergence des suites arithmético-géométriques définies par :

- 1. $u_0 = 0$ et $u_{n+1} = 2u_n - 1$;
- 2. $u_0 = 1$ et $u_{n+1} = -\frac{1}{2}u_n + 1$.

2.14. Soit (u_n) la suite définie par $u_0 = 0$, $u_1 = 1$ et $u_{n+1} = \frac{1}{2}(u_n + u_{n-1})$ pour $n \geq 1$.

- 1. Placer quelques termes de cette suite sur le segment $[0; 1]$.
- 2. On pose $v_n = u_n - u_{n-1}$ pour $n \geq 1$.
Montrer que la suite (v_n) est géométrique, puis calculer son terme général.
- 3. Calculer $S_n = v_1 + \dots + v_n$ et en déduire u_n .
- 4. Calculer la limite de la suite (u_n) .

2.15. Soit (u_n) une suite à termes strictement positifs.

- 1. Supposons qu'il existe $k \in]0; 1[$ tel que $\frac{u_{n+1}}{u_n} \leq k$ à partir d'un certain rang. Montrer qu'alors la suite (u_n) converge vers 0.
- 2. Supposons que $\lim_{n \rightarrow +\infty} \frac{u_{n+1}}{u_n} = \ell < 1$. Montrer qu'alors la suite (u_n) converge vers 0.
- 3. Application. Déterminer la limite de la suite de terme général $\frac{n^{1789}}{n!}$.

Limites

On se référera principalement au chapitre 1.

2.16. Calculer les limites des suites définies par :

1. $u_n = \frac{2n+1}{3n-5}$;

2. $u_n = \frac{-4n^2 + 3n + 3}{n^2 - n + 4}$;

3. $u_n = \frac{4^n - 3^n}{4^n + 2^n}$;

4. $u_n = 2n - \sqrt{4n^2 - 3n + 1}$;

5. $u_n = \sin \frac{1}{n^2}$;

6. $u_n = \sqrt{3^n - 2^n}$.

2.17. Soit (x_n) la suite définie par $x_n = 2^{2^n} \sin 2^{-2^n}$. Étudier la limite de (x_n) sur un tableur puis conclure rigoureusement.

Démonstration par récurrence

2.18. Montrer que la proposition « 9 divise $10^n + 1$ » est héréditaire. Est-elle vraie ?

2.19. Montrer que, pour tout $n \geq 0$, $\sum_{k=0}^n 2^k = 2^{n+1} - 1$. Quelle est la traduction évidente de ce résultat en binaire ?

2.20. Montrer que $2^n \geq n^2$ à partir d'un rang qu'on déterminera.

2.21. Soit (u_n) la suite définie par $u_0 = 1$ et $u_{n+1} = u_n + 2n + 3$. Conjecturer puis prouver l'expression de son terme général u_n en fonction de n .

2.22. Montrer que $\sum_{k=1}^n k^3 = \left(\sum_{k=1}^n k \right)^2$.

Étude de suites récurrentes

2.23. Soit f la fonction définie sur $[-2; +\infty[$ par $f(x) = \sqrt{x+2}$.

1. Déterminer le sens de variation de f .

2. Soit (u_n) la suite définie par $u_{n+1} = f(u_n)$ et $u_0 = -1$.

(a) Que peut-on penser de la suite (u_n) ?

(b) Montrer que $-2 \leq u_n \leq u_{n+1} \leq 2$ pour tout n .

(c) Quel est le sens de variation de (u_n) ?

3. Soit (v_n) la suite définie par $v_{n+1} = f(v_n)$ et $v_0 = 7$.

(a) Que peut-on penser de la suite (v_n) ?

(b) Montrer que $2 \leq v_{n+1} \leq v_n \leq 7$ pour tout n .

(c) Quel est le sens de variation de (v_n) ?

4. Peut-on déduire le sens de variation d'une suite récurrente du sens de variation de la fonction associée ?

5. (a) Montrer que les suites (u_n) et (v_n) convergent.

(b) Déterminer leurs limites.

2.24. Soit (u_n) une suite récurrente, définie par u_0 et $u_{n+1} = f(u_n)$. On suppose que la fonction f est croissante et que $u_0 \leq u_1$. Montrer que (u_n) est croissante.

2.25. Soit (u_n) la suite définie par $u_0 = \frac{1}{4}$ et $u_{n+1} = \frac{2 + 3u_n}{4 + u_n}$.

1. Observer le comportement de (u_n) sur un tableur. Quelles conjectures peut-on faire ?

2. Construire graphiquement les premiers termes de (u_n) . Quelles sont les valeurs possibles de l'éventuelle limite de (u_n) ?

3. Montrer que la suite (v_n) de terme général $\frac{2 + u_n}{1 - u_n}$ est géométrique.

4. En déduire l'expression de u_n puis sa limite. Pourrait-on déterminer cette limite sans passer par l'expression du terme général ?

2.26. Soient (u_n) et (v_n) les suites définies par $u_0 = 12$ et $u_{n+1} = \frac{u_n + 2v_n}{3}$, $v_0 = 1$ et $v_{n+1} = \frac{u_n + 3v_n}{4}$.

1. Observer le comportement de ces deux suites sur un tableur. Quelles conjectures peut-on faire ? Expliquer comment construire géométriquement les termes de ces suites sur la droite réelle.

2. Montrer que la suite (w_n) définie par $w_n = u_n - v_n$ est géométrique.

3. Montrer que (u_n) et (v_n) sont adjacentes.

4. Peut-on déduire leur limite commune des relations de récurrence les définissant ?

5. Montrer que la suite (t_n) définie par $t_n = 3u_n + 8v_n$ est constante.

6. En déduire les termes généraux de (u_n) et (v_n) , puis leur limite.

Suites définies par des sommes

2.27. Soit (u_n) la suite définie pour $n \geq 1$ par $u_n = \sum_{k=1}^n \frac{1}{k(k+1)}$.

1. Déterminer les réels a et b tels que $\frac{1}{k(k+1)} = \frac{a}{k} + \frac{b}{k+1}$.

2. En déduire la limite de (u_n) .

2.28. Montrer par majoration que la suite de terme général $\sum_{k=1}^n \frac{1}{(n+k)^2}$ tend vers 0.

2.29. Montrer que $\frac{1}{\sqrt{k}} \geq 2(\sqrt{k+1} - \sqrt{k})$ et en déduire que la suite de terme général $\sum_{k=1}^n \frac{1}{\sqrt{k}}$ tend vers $+\infty$.

3. Continuité

3.1 Généralités

Définition. Soit f une fonction définie sur un intervalle I contenant le réel a . Alors :

- la fonction f est *continue* en a si $\lim_{x \rightarrow a} f(x) = f(a)$;
- la fonction f est *continue* sur I si elle est continue en tout point de I .

Remarque. Concrètement, f est continue ssi l'on peut tracer son graphe sans lever le crayon (*connexité par arcs*).

Théorème. Sous certaines conditions d'existence, la somme, le produit, le quotient et la composée de deux fonctions continues sont continus.

Preuve. Il s'agit d'une conséquence directe des théorèmes d'opération sur les limites.

Par exemple la composée : supposons (en mettant de côté la rigueur maniaque) que f est continue en a et g en $f(a)$. Alors par définition, $\lim_{x \rightarrow a} f(x) = f(a)$ et $\lim_{y \rightarrow f(a)} g(y) = g(f(a))$. Le théorème de composition des limites donne $\lim_{x \rightarrow a} g(f(x)) = g(f(a))$. \square

Théorème. Les fonctions puissances, polynômes, racine carrée et valeur absolue sont continues leurs ensembles de définition.

Preuve. • La fonction identité est trivialement continue, donc $x^n = x \times x \times \dots \times x$ aussi (récurrence). Par suite, un monôme $a_n x^n$ est continu et finalement un polynôme $a_n x^n + \dots + a_1 x + a_0$ aussi.

- On remarque que $|\sqrt{x} - \sqrt{a}| = \frac{|x - a|}{\sqrt{x} + \sqrt{a}} \leq \frac{|x - a|}{\sqrt{a}}$ a pour limite 0 lorsque $x \rightarrow a$. Ainsi $\lim_{x \rightarrow a} \sqrt{x} = \sqrt{a}$ et donc la fonction racine carrée est continue en $a \neq 0$.
- La relation $|x| = \sqrt{x^2}$ montre que la fonction valeur absolue est continue.

\square

Bien que l'immense majorité des fonctions traitées en terminale soient continues (et même dérivables), certaines ne le sont pas :

Exemple. La fonction partie entière $\lfloor x \rfloor$ est *discontinue* en tout x entier.

3.2 Théorème des valeurs intermédiaires

3.2.1 Existence

Théorème. Soit f une fonction continue sur un intervalle I , et soient a et b deux points de I . Pour tout réel k compris entre $f(a)$ et $f(b)$, il existe un réel c compris entre a et b vérifiant $f(c) = k$.

Preuve. Supposons $a < b$ et, quitte à considérer $-f$, $f(a) < k < f(b)$. On procède par dichotomie. On pose $I_0 = [a; b]$. On prend ensuite $I_1 = \left[\frac{a+b}{2}; b\right]$ si $f\left(\frac{a+b}{2}\right) \leq k$, ou $I_1 = \left[a; \frac{a+b}{2}\right]$ sinon. On pose $I_n = [a_n; b_n]$. Cette suite dichotomique d'intervalles converge vers un réel $c = \lim_{n \rightarrow +\infty} a_n = \lim_{n \rightarrow +\infty} b_n$; de plus, par construction, $f(a_n) \leq k \leq f(b_n)$. En passant à la limite dans cette inégalité, la continuité de f montre que $f(c) \leq k \leq f(c)$, soit $f(c) = k$. \square

Remarque. Ici le nombre c n'est pas nécessairement unique. L'algorithme de dichotomie converge vers une solution, et l'on ne peut savoir *a priori* laquelle sans préciser la fonction.

Corollaire. L'image d'un intervalle par une fonction continue est un intervalle.

Preuve. Soient x et y deux éléments de $f(I)$. On doit montrer que tout z vérifiant $x < z < y$ est encore dans $f(I)$ (propriété caractéristique des intervalles). On observe qu'il existe a et b dans I tels que $x = f(a)$ et $y = f(b)$. Le théorème des valeurs intermédiaires prouve qu'il existe c dans I avec $z = f(c)$. Par conséquent $z \in f(I)$. \square

3.2.2 Unicité

Théorème. Soit f une fonction continue et strictement monotone sur un intervalle I , et soient a et b deux points de I .

Pour tout réel k compris entre $f(a)$ et $f(b)$, il existe un unique réel c compris entre a et b vérifiant $f(c) = k$.

Preuve. L'équation $f(c) = k$ possède au moins une solution par le théorème d'existence. La stricte monotonie de f montre que c est unique : $f(c_1) = k = f(c_2)$ avec $c_1 < c_2$ contredit $f(c_1) < f(c_2)$ ou $f(c_1) > f(c_2)$. \square

3.2.3 En pratique

Limites

Le théorème des valeurs intermédiaires peut s'appliquer aussi sous forme étendue. Par exemple, considérons $f(x) = x^3$. On sait que $f(0) = 0$ et $\lim_{x \rightarrow +\infty} f(x) = +\infty$. Puisque f est continue et strictement croissante sur \mathbb{R}_+ , il existe un unique réel positif c vérifiant $f(c) = 2^{1789} + \sqrt{1515}$.

Mémento

Lorsque l'on souhaite appliquer le théorème des valeurs intermédiaires, il ne faut *jamais* oublier les points suivants :

- continuité ;
- stricte monotonie (si l'on veut montrer l'unicité) ;
- valeurs.

Grapher et tableur

Imaginons maintenant que l'on demande un encadrement de la racine α de $g(x) = x^3 - 2$ d'amplitude 0,01. On trace g entre 0 et 2 (intervalle sûr) sur un grapheur. La fonction trace ou un tableur (avec un pas de 0,01) montre que $g(1,25) < 0$ et $g(1,26) > 0$. Puisque g est continue et strictement croissante, le théorème des valeurs intermédiaires prouve $1,25 < \alpha < 1,26$. Il serait bien trop long, à la main, de faire une dichotomie.

3.2.4 Algorithme

La preuve du théorème des valeurs intermédiaires fournit de manière tautologique un algorithme. En n étapes, il permet de donner un encadrement de c d'amplitude $\frac{b-a}{2^n}$. La convergence est donc rapide.

3.3 Compléments

3.3.1 Bijection

Définition. Soit f une fonction définie sur un ensemble A , à valeurs dans un ensemble B . La fonction f est une *bijection* de A sur B si, pour tout $y \in B$, il existe un unique $x \in A$ tel que $f(x) = y$. La fonction qui associe y à x est alors la *bijection réciproque* de f , notée f^{-1} .

Remarque. Autrement dit, pour tout y dans B , l'équation $f(x) = y$ possède une unique solution dans A . On a alors l'équivalence $f(x) = y \Leftrightarrow x = f^{-1}(y)$.

Théorème. Soit f une bijection de I sur J , ces ensembles étant des intervalles réels. Soient \mathcal{C} et \mathcal{C}^{-1} les courbes représentatives de f et f^{-1} dans un repère orthonormal. Alors \mathcal{C} et \mathcal{C}^{-1} sont symétriques par rapport à la première bissectrice.

Preuve. L'idée est essentiellement que la symétrie par rapport à la première bissectrice transforme un point de coordonnées $(x; y)$ en un autre de coordonnées $(y; x)$. □

En pratique, le résultat suivant permet de prouver facilement une bijectivité :

Théorème. Une fonction continue et strictement monotone sur un intervalle I réalise une bijection de I sur $f(I)$.

Preuve. Tous les éléments de $f(I)$ possèdent par définition au moins un antécédent par f . Il est unique car f est strictement monotone. □

3.3.2 Fonctions continues sur un segment

Rappelons qu'un *segment* est un intervalle fermé borné.

Théorème. Une fonction continue sur un segment est bornée.

Preuve. Soit f une fonction continue sur un segment $[a; b]$. On va montrer que f est majorée ; sa minoration se démontre identiquement. Raisonnons par l'absurde et supposons que f n'est pas majorée sur $[a; b]$. Définissons une dichotomie de $[a; b]$. On pose $I_0 = [a; b]$, puis on définit $I_1 = \left[a; \frac{a+b}{2} \right]$ si f n'y est pas majorée et $I_1 = \left[\frac{a+b}{2}; b \right]$ sinon. Ainsi, sur chaque I_n , f n'est pas majorée. La suite (I_n) converge vers un réel c . Puisque f est continue en c , si x est assez proche de c , $f(x)$ est assez proche de $f(c)$, donc en particulier f est majorée sur un voisinage V assez étroit de c . Si n est assez grand, $I_n \subset V$ car (I_n) converge vers c . Or f n'est pas majorée sur I_n , ce qui est en contradiction avec la majoration de f sur V . \square

On dispose en fait d'un résultat plus précis :

Théorème. Une fonction continue sur un segment possède un maximum et un minimum.

Preuve. Soit f une fonction continue sur un segment $I = [a; b]$. On va montrer que f possède un maximum ; l'existence d'un minimum se prouve identiquement. On rappelle que l'image d'un segment par f est un intervalle, que l'on sait borné grâce au théorème précédent. On a donc $J = f(I) =]m; M]$. Si M est inclus dans J , c'est nécessairement un maximum. Supposons donc qu'il n'est pas inclus i.e. $J =]m; M[$. On réalise encore une dichotomie de $[a; b]$. On pose $I_0 = [a; b]$ puis $I_1 = \left[a; \frac{a+b}{2} \right]$ ou $I_1 = \left[\frac{a+b}{2}; b \right]$ en choisissant celui (ou l'un) dont l'intervalle image par f a pour borne supérieure le réel M . La suite (I_n) converge vers un réel $c \in I$. Si $f(c) < M$, alors la continuité de f montre qu'il existe un voisinage V de c tel que $f(V)$ soit majoré par $\frac{f(c) + M}{2}$. Pour n assez grand, on a $I_n \subset V$. Or la borne supérieure de $f(I_n)$ vaut M , plus grande que celle de $f(V)$, ce qui est absurde. \square

3.4 Exercices

Généralités

3.1. Soient f et g deux fonctions continues définies sur un intervalle I .

1. Vérifier que $\max(f, g) = \frac{|f - g| + f + g}{2}$.

2. En déduire que la fonction $\max(f, g)$ est continue.

3.2. Soit f la fonction définie sur \mathbb{R} par $f(x) = 4x + 2$ si $x \leq -1$ et $f(x) = x^2 + bx + c$ si $x > -1$. Trouver b et c tels que f soit dérivable et f' soit continue.

Théorème des valeurs intermédiaires

3.3. Soit f la fonction définie sur \mathbb{R} par $f(x) = x^5 + x^3 + x + 1$. Montrer que f possède une unique racine.

3.4. Montrer que tout polynôme de degré impair possède au moins une racine réelle.

3.5. Soit P la fonction définie sur \mathbb{R} par $P(x) = x^3 + x^2 - 3x + 1$.

1. Dresser le tableau de variations de P .

2. En déduire le nombre de racines de P .

3. Retrouver directement ces racines en factorisant $P(x)$.

3.6. Soit f la fonction définie sur \mathbb{R}_+ par $f(x) = x^2 + \sqrt{x} - 3$. Montrer que f possède une unique racine puis en donner un encadrement d'amplitude 0,01.

3.7. Soit $f : [0; 1] \rightarrow [0; 1]$ une fonction continue. Montrer que f possède au moins un point fixe.

3.8. Montrer qu'une fonction continue sur \mathbb{R} qui ne s'annule jamais est de signe constant.

Compléments

3.9. Montrer que la fonction puissance n -ième définie sur \mathbb{R}_+ par $f(x) = x^n$ ($n \in \mathbb{N}^*$) réalise une bijection de \mathbb{R}_+ sur \mathbb{R}_+ . On appelle fonction *racine n -ième* sa réciproque.

3.10. Soit f la fonction définie sur $[0; 1]$ par $f(x) = x - 2\sqrt{x} + 1$. Montrer que f réalise une bijection de $[0; 1]$ sur $[0; 1]$. Montrer que $f = f^{-1}$ (f est *involutive*).

3.11. Soit g la fonction définie par $g(x) = \frac{x}{1 + |x|}$. Montrer que g réalise une bijection de \mathbb{R} sur $] -1; 1[$. Démontrer que $g^{-1}(x) = \frac{x}{1 - |x|}$ pour tout x de $] -1; 1[$.

4. Dérivation

4.1 Généralités

4.1.1 Définitions

Définition. Soit f une fonction définie sur un intervalle I . Soit $a \in I$.

- La fonction f est *dérivable* en a s'il existe une fonction ε vérifiant $\lim_{h \rightarrow 0} \varepsilon(h) = 0$ et un réel λ tels que

$$f(a+h) = f(a) + \lambda h + h\varepsilon(h).$$

- Le nombre λ est le *nombre dérivé* de f en a , noté $f'(a)$.
- Si f est dérivable en tout point de I , alors la fonction f est *dérivable* sur I , et f' est la *fonction dérivée* de f .

Remarque. Si f est dérivable en a alors $f(a+h) = f(a) + f'(a)h + h\varepsilon(h)$.

Théorème. Cette définition est équivalente à

$$\lim_{h \rightarrow 0} \frac{f(a+h) - f(a)}{h} = \lambda.$$

Preuve. $\lim_{h \rightarrow 0} \frac{f(a+h) - f(a)}{h} = \lambda \Leftrightarrow \frac{f(a+h) - f(a)}{h} = \lambda + \varepsilon(h)$ avec $\lim_{h \rightarrow 0} \varepsilon(h) = 0$ d'où le résultat en multipliant par h . □

Corollaire. Le réel λ de la définition est donc unique.

Remarque. Si h est petit, on a $f(a+h) \approx f(a) + f'(a)h$. C'est l'*approximation affine* de f en a , obtenue en négligeant l'*erreur* constituée par $h\varepsilon(h)$.

Dans la suite, une fonction notée ε tendra vers 0 en 0.

4.1.2 Continuité

Théorème. Soit f une fonction définie sur un intervalle I , et soit $a \in I$.

Si f est dérivable en a alors f est continue en a .

Preuve. Si f est dérivable en a alors $f(x) = f(a) + f'(a)(x-a) + (x-a)\varepsilon(x-a)$, qui a pour limite $f(a) + f'(a) \times 0 + 0 \times 0 = f(a)$ lorsque x tend vers a . □

Corollaire. Si f n'est pas continue en a alors elle n'est pas dérivable en a .

En pratique, on pourra faire d'une pierre deux coups en montrant qu'une fonction est dérivable, si par exemple on a besoin de ses variations et de sa continuité.

Une fonction continue n'est pas nécessairement dérivable, comme le prouve la fonction valeur absolue. En général, disons dans les cas simples, une fonction est dérivable si sa courbe ne recèle pas d'angles (ce qui empêche l'existence d'une tangente).

4.1.3 Tangente

Théorème. Soit f une fonction définie sur un intervalle I . Si f est dérivable en a , alors \mathcal{C}_f possède une tangente en $A(a; f(a))$ d'équation $y - f(a) = f'(a)(x - a)$.

Preuve. Pour se souvenir de cette formule sans avoir recours à des moyens illicites, il suffit de se placer dans le repère $(A; \vec{i}, \vec{j})$ (i.e. faire un changement de variables). La tangente passe par l'origine A et sa pente vaut $f'(a)$; son équation est donc $Y = f'(a)X$. Or, $x = a + X$ et $y = f(a) + Y$, ce qui amène au résultat souhaité. \square

Remarque. L'équation de la tangente $y = f(a) + f'(a)(x - a)$ n'est autre que l'approximation affine de f en a .

4.1.4 Notation différentielle et cinématique

- On peut écrire, sous forme pratique, l'expression de la dérivée par

$$\Delta y = f'(x)\Delta x + \Delta x.\varepsilon(\Delta x).$$

Mettons la rigueur de côté. Si Δx est infiniment petit, alors Δy aussi, et on les note dx et dy (*notations différentielles*). Puisque la limite en 0 de ε vaut 0, on a donc $dy = f'(x) dx$.

On peut donc écrire également $\frac{dy}{dx} = f'(x)$.

- Soit $x(t)$ la position d'un mobile. On a alors :

- sa vitesse $v(t) = x'(t) = \frac{dx}{dt} = \dot{x}$;

- son accélération $\gamma(t) = v'(t) = x''(t) = \frac{d}{dt} \frac{dx}{dt} = \frac{d^2x}{dt^2} = \ddot{x}$.

4.2 Opérations

4.2.1 Somme, produit, quotient

On rappelle les résultats suivants :

Théorème. Soient f et g deux fonctions dérivables sur un intervalle I .

- $f + g$ est dérivable sur I , et sa dérivée vaut $(f + g)' = f' + g'$;
- fg est dérivable sur I , et sa dérivée vaut $(fg)' = f'g + fg'$;
- $\frac{f}{g}$ est dérivable sur I lorsque g' ne s'annule pas, et sa dérivée vaut $\left(\frac{f}{g}\right)' = \frac{f'g - fg'}{g^2}$.

4.2.2 Composée

Théorème. Soit f une fonction définie sur un intervalle I , et soit x_0 un point de I . Soit g une fonction définie sur un intervalle J contenant $y_0 = f(x_0)$.

Si f est dérivable en x_0 et g en y_0 alors la composée $g \circ f$, définie par $(g \circ f)(x) = g(f(x))$, est dérivable en x_0 avec

$$(g \circ f)'(x_0) = f'(x_0)g'(f(x_0)).$$

Preuve. On peut écrire $\frac{g(f(x)) - g(f(x_0))}{x - x_0} = \frac{g(y) - g(y_0)}{y - y_0} \frac{f(x) - f(x_0)}{x - x_0}$, produit de taux d'accroissements qui a pour limite $g'(y_0)f'(x_0)$ lorsque x tend vers x_0 . Malheureusement $y - y_0 = f(x) - f(x_0)$ peut s'annuler même lorsque x est infiniment proche de x_0 , ce qui n'est absolument pas virtuel (par exemple le graphe de $x^2 \sin \frac{1}{x}$ recoupe infiniment l'axe des abscisses au voisinage de 0). On peut cependant contourner ce problème en posant $h(y) = \frac{g(y) - g(y_0)}{y - y_0}$ si $y \neq y_0$ et $h(y_0) = g'(y_0)$. On a alors $\frac{g(f(x)) - g(f(x_0))}{x - x_0} = h(y) \frac{f(x) - f(x_0)}{x - x_0}$, qui a bien pour limite $g'(y_0)f'(x_0)$. \square

Remarque. • On écrit souvent ce résultat sous la forme pratique $f(u)' = u'f'(u)$.

- Dans la lignée de cette preuve, on dispose de la règle de Leibniz (*chain rule* en anglais) :

$$\frac{dz}{dx} = \frac{dz}{dy} \frac{dy}{dx}$$

que tout le monde adore pour sa simplicité et sa commodité.

Corollaire. Soit u une fonction dérivable en x_0 . On a les formules de dérivabilité suivantes :

- $(u^n)' = nu'u^{n-1}$ pour $n \in \mathbb{Z}$ et u si besoin non nul ;
- $(\sqrt{u})' = \frac{u'}{2\sqrt{u}}$ pour $u > 0$.

Preuve. Il suffit d'appliquer la formule $f(u)' = u'f'(u)$ pour $f(x) = x^n$ puis $f(x) = \sqrt{x}$. \square

4.3 Variations

Théorème. Soit f une fonction dérivable sur un intervalle I .

- Si $f' \geq 0$ (resp. > 0) alors f est (resp. strictement) croissante sur I ;
- Si $f' \leq 0$ (resp. < 0) alors f est (resp. strictement) décroissante sur I ;
- Si $f' = 0$ alors f est constante sur I .

Remarque. • Ce théorème a été admis en première et est également admis en terminale car assez délicat (voir les compléments des exercices pour une preuve basée sur le théorème des accroissements finis).

- Lors d'une étude classique de fonction, l'obtention du tableau de variation s'obtient en résolvant par exemple l'inéquation $f' \geq 0$; la résolution de $f' = 0$ est insuffisante car elle ne fournit pas le *signe* de f' .
- Si f' est > 0 (resp. < 0) à l'exception de points isolés où $f' = 0$ alors f est néanmoins toujours strictement croissante (resp. décroissante).

Théorème. Soit f une fonction dérivable sur un intervalle I , et soit x_0 intérieur à I .

- Si f admet un extremum local en x_0 alors $f'(x_0) = 0$.
- Si f' s'annule en changeant de signe en x_0 alors f admet un extremum local en x_0 .

Preuve.

- On sait que $f'(x_0) = \lim_{x \rightarrow x_0} \frac{f(x) - f(x_0)}{x - x_0}$. Supposons par exemple que $f(x_0)$ soit un maximum local. Pour x dans un voisinage de x_0 , on a donc $f(x) < f(x_0)$. Par conséquent $\frac{f(x) - f(x_0)}{x - x_0}$ y est positif si $x < x_0$ et négatif si $x > x_0$. La limite à gauche de ce taux d'accroissement est donc positive et la limite à droite négative. La limite $f'(x_0)$ est donc positive et négative i.e. nulle.
- Supposons par exemple que, dans un voisinage $]x_0 - \varepsilon; x_0 + \varepsilon[$ de x_0 , f' soit positive sur $]x_0 - \varepsilon; x_0[$ puis négative sur $]x_0; x_0 + \varepsilon[$. Ainsi f est croissante puis décroissante et finalement $f(x_0)$ est un maximum local.

□

Remarque.

- Les extremums locaux sont donc à rechercher parmi les zéros de la dérivée.
- Être un zéro de la dérivée ne suffit pas à être un extremum local (par exemple x^3 en 0).
- En pratique, on fera souvent un tableau de variation afin de faire apparaître les extremums locaux (ou globaux).

4.4 Exercices

Généralités

4.1. Montrer que la fonction f définie sur \mathbb{R} par $f(x) = 1 + 3x - 1789x \sin x$ est dérivable en 0 et calculer son nombre dérivé.

4.2. Montrer que la fonction f définie sur \mathbb{R} par $f(x) = 1 - 7x + x|x|$ est dérivable en 0 et calculer son nombre dérivé.

4.3. Montrer que la fonction valeur absolue n'est pas dérivable en 0.

4.4. 1. Montrer que la dérivée d'une fonction dérivable paire (resp. impaire) est impaire (resp. paire).

2. Établir une réciproque.

4.5. Soit f une fonction dérivable en a avec $f'(a) \neq 0$. Montrer que la tangente à \mathcal{C}_f en $A(a; f(a))$ coupe l'axe des abscisses en un point d'abscisse $a - \frac{f(a)}{f'(a)}$.

4.6. En supposant que les objets existent, montrer que $(f^{-1})'(x) = \frac{1}{f'(f^{-1}(x))}$.

4.7. Montrer que la tangente à l'hyperbole équilatère $y = \frac{1}{x}$ en un point M coupe les axes en deux points symétriques par rapport à M .

Calculs de dérivées

Dans cette section, on ne demande pas de justifier l'existence ou la dérivabilité des fonctions proposées.

4.8. Dériver les fonctions suivantes :

1. $1 + x + \frac{x^2}{2} + \frac{x^3}{3!} + \frac{x^4}{4!}$;

2. $x\sqrt{x}$;

3. $\frac{\sqrt{x}}{1+x}$;

4. $\frac{ax+b}{cx+d}$.

4.9. Dériver les fonctions suivantes :

1. $(2x+1)^3$;

2. $\sqrt{2x^2+x}$.

Études de fonctions

4.10. Trouver sur \mathbb{R} les extremums locaux de $f(x) = x^3 - 6x^2 + 1$. Sont-ils globaux ?

4.11. Étudier la fonction f définie sur $\mathbb{R} - \{2\}$ par $f(x) = x - 1 + \frac{1}{x-2}$.

4.12. Soit f la fonction définie sur \mathbb{R} par $f(x) = \frac{x}{1+x^2}$.

1. Montrer que f est impaire.
2. Étudier les variations de f .
3. Montrer que la courbe de f possède trois *points d'inflexion* i.e. des points M_0 d'abscisse x_0 telle que f'' s'y annule en changeant de signe.
Si $f'' > 0$ la fonction est convexe et si $f'' < 0$ la fonction est concave.

Divers

4.13. Soit f la fonction définie sur $[0; 1]$ par $f(x) = x - 2\sqrt{x} + 1$. La courbe de f est-elle un arc de cercle ?

4.14. Soit f la fonction définie sur $[-1; 1]$ par $f(x) = \sqrt{1-x^2}$.

1. Montrer que \mathcal{C}_f est un demi-cercle.
2. Déterminer l'équation de la tangente à \mathcal{C}_f au point d'abscisse x_0 .

4.15. On considère, suivant un modèle dépassé, que la trajectoire de l'électron de l'atome d'hydrogène est un cercle de rayon $r = 3.10^{-11}\text{m}$. On rappelle que l'intensité de la *force électrostatique* F entre deux charges électriques q et q' est donnée par $F = \frac{kqq'}{r^2}$ où $k = 9.10^9$ unités SI. La *charge élémentaire* de l'électron est $e = 1,6.10^{-19}\text{C}$. Calculer une valeur approchée de la variation de la force électrostatique entre l'électron et le noyau de l'atome d'hydrogène quand r varie de $\Delta r = 2.10^{-13}\text{m}$.

4.16. En mécanique relativiste, la masse m d'un corps en mouvement est donnée en fonction de sa vitesse v par $m = m_0/\sqrt{1 - \frac{v^2}{c^2}}$, où c est la vitesse de la lumière et m_0 la masse du corps au repos. Dans ces conditions, l'énergie cinétique E est donnée par $E = (m - m_0)c^2$. On se propose de montrer que, pour $\frac{v}{c}$ suffisamment petit, une valeur approchée de E est $\frac{1}{2}m_0v^2$, ce qui correspond à la formule de l'énergie cinétique en mécanique classique.

1. Que signifie physiquement « $\frac{v}{c}$ petit » ?
2. On pose $x = \left(\frac{v}{c}\right)^2$. Montrer que $E = m_0c^2 \left(\frac{1}{\sqrt{1-x}} - 1 \right)$.
3. Soit f la fonction définie sur $[0; 1[$ par $f(x) = \frac{1}{\sqrt{1-x}} - 1$. Montrer que f est dérivable, puis écrire l'approximation affine de f en 0.
4. Établir le résultat annoncé. Obtient-on au passage une estimation de l'erreur commise ?

Compléments

4.17. Soit f une fonction dérivable sur $[a; b]$. On suppose que $p \leq f'(x) \leq q$.

1. Montrer que la fonction φ définie par $\varphi(x) = f(x) - px$ est croissante.

2. En déduire que $\frac{f(b) - f(a)}{b - a} - p \geq 0$.

3. Établir l'encadrement des accroissements finis $p \leq \frac{f(b) - f(a)}{b - a} \leq q$.

4.18. Soit f une fonction dérivable sur $[a; b]$. On suppose que $|f'(x)| \leq M$.

1. Établir l'inégalité des accroissements finis $|f(b) - f(a)| \leq M(b - a)$.

2. Quelle est la distance maximale qu'un véhicule ne dépassant pas 130km/h peut parcourir en une heure ?

4.19. Soit f une fonction dérivable sur $[a; b]$ dont la dérivée est elle-même continue (f est de classe C^1).

1. Montrer que f' possède un minimum $f'(\alpha)$ et un maximum $f'(\beta)$. Déduire d'un des résultats vus précédemment que $f'(\alpha) \leq \frac{f(b) - f(a)}{b - a} \leq f'(\beta)$.

2. Montrer en appliquant le théorème des valeurs intermédiaires qu'il existe $c \in [a; b]$ tel que $f(b) - f(a) = f'(c)(b - a)$ (égalité des accroissements finis).

3. Retrouver dans ce cas qu'une fonction dont la dérivée est strictement positive est strictement croissante.

Ce résultat est plus subtil à prouver dans le cas où f est simplement dérivable.

4.20. On réalise un ensemble $\mathcal{M} = \{M_k = (i_k; u_k), 1 \leq k \leq n\}$ de mesures de tension et intensité aux bornes d'une résistance r inconnue, que l'on rappelle soumise à la loi d'Ohm $u = ri$. On souhaite donner la meilleure valeur de r au sens des *moindres carrés*. Pour cela, on place notre nuage \mathcal{M} de points et on cherche a tel que la droite linéaire $\Delta : y = ax$ minimise la somme $S(a)$ des carrés des distances des points M_k de \mathcal{M} à leur projeté vertical H_k sur Δ .

1. Montrer que $H_k M_k^2 = (u_k - ai_k)^2$ et en déduire que $S(a) = \sum_{k=1}^n (u_k - ai_k)^2$.

2. Montrer que $S(a)$ est une fonction polynômiale du second degré de coefficient dominant positif.

3. En déduire la valeur de a qui répond au problème.

Cette valeur est la pente de la droite de régression linéaire.

4.21. Soit f un polynôme de degré $n \geq 2$. On dit que x_0 est une *racine d'ordre p* de f s'il existe un polynôme g vérifiant $f(x) = (x - x_0)^p g(x)$ avec $g(x_0) \neq 0$, quel que soit x dans \mathbb{R} .

1. Montrer que x_0 est une racine d'ordre 1 (dite *simple*) ssi $f(x_0) = 0$ et $f'(x_0) \neq 0$.

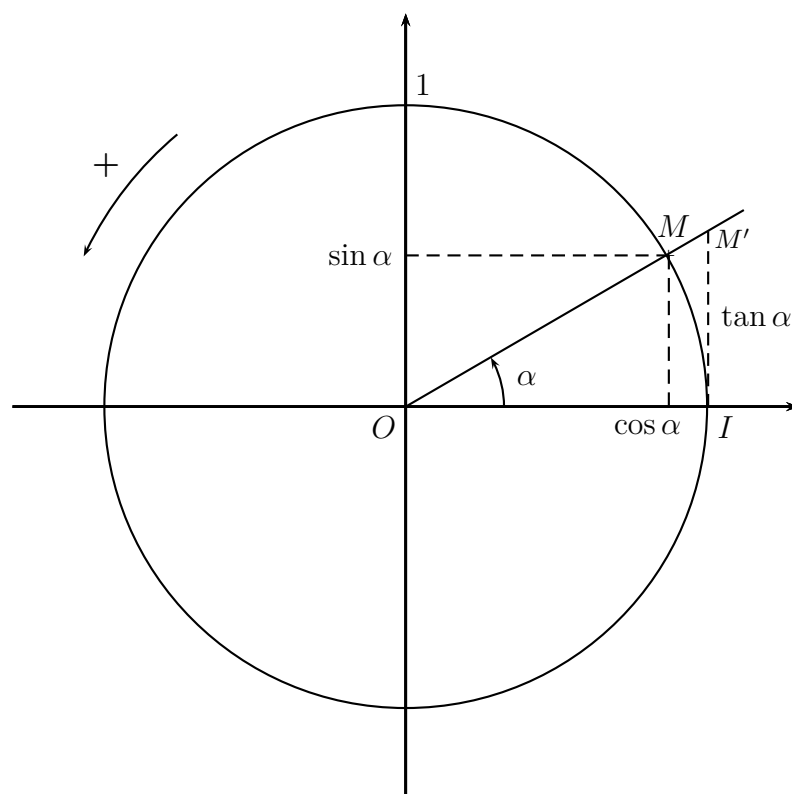
2. Montrer que x_0 est une racine d'ordre 2 (dite *double*) ssi $f(x_0) = f'(x_0) = 0$ et $f''(x_0) \neq 0$.

(a) Retrouver les conditions pour qu'un polynôme du second degré possède une racine double.

(b) Soit $f(x) = x^3 + px + q$. Montrer qu'une condition nécessaire et suffisante pour que f admette une racine double est $4p^3 + 27q^2 = 0$ et $p \neq 0$.

5. Fonctions trigonométriques

5.1 Cercle trigonométrique



Quelques rappels géométriques :

- Le *cercle trigonométrique* est le cercle de centre O et de rayon 1, orienté comme indiqué.
- La mesure $\alpha \in [0; 2\pi[$ (en radians) de l'angle \widehat{IOM} est par définition la mesure de l'arc de cercle \widehat{IM} .
- Si $M(x; y)$ est un point de ce cercle associé à un angle α alors par définition $x = \cos \alpha$ et $y = \sin \alpha$.
- La *tangente* $\tan \alpha = \frac{\sin \alpha}{\cos \alpha}$ peut s'interpréter comme la pente de la droite (OM) , qui est aussi la distance indiquée IM' sur le dessin.

Définition.

- La fonction qui, à $\alpha \in \mathbb{R}$, associe $\cos \alpha$, est la *fonction cosinus*.
- La fonction qui, à $\alpha \in \mathbb{R}$, associe $\sin \alpha$, est la *fonction sinus*.

5.2 Dérivabilité

5.2.1 Résultats préparatoires

Lemme. Pour un petit angle $\alpha > 0$, on a $\sin \alpha \leq \alpha \leq \tan \alpha$.

Preuve. On a clairement $\text{aire}(OMI) \leq \text{aire}(\widehat{IOM}) \leq \text{aire}(OM'I)$, ce qui se traduit par

$$\frac{1 \cdot \sin \alpha}{2} \leq \frac{\alpha}{2\pi} \pi \cdot 1^2 \leq \frac{1 \cdot \tan \alpha}{2}.$$

Le résultat souhaité est obtenu par simplification évidente. \square

Lemme. La fonction cosinus est continue en 0.

Preuve. La longueur de la corde $[IM]$ est inférieure ou égale à la longueur de l'arc \widehat{IM} . Ainsi $\sqrt{\sin^2 \alpha + (1 - \cos \alpha)^2} \leq \alpha$, soit $\sqrt{2 - 2 \cos \alpha} \leq \alpha$. On passe au carré : $2 - 2 \cos \alpha \leq \alpha^2$, ce qui donne $\cos \alpha \geq 1 - \frac{\alpha^2}{2}$. Finalement $1 - \frac{\alpha^2}{2} \leq \cos \alpha \leq 1$. Le théorème d'encadrement prouve alors que $\cos \alpha$ tend vers $1 = \cos 0$ lorsque α tend vers 0^+ . \square

Lemme. On a $\lim_{\alpha \rightarrow 0} \frac{\sin \alpha}{\alpha} = 1$.

Preuve. Soit $\alpha > 0$. On sait alors que $\sin \alpha \leq \alpha \leq \tan \alpha = \frac{\sin \alpha}{\cos \alpha}$, ce qui donne d'une part $\frac{\sin \alpha}{\alpha} \leq 1$ et d'autre part $\frac{\sin \alpha}{\alpha} \geq \cos \alpha$. Il vient donc $\cos \alpha \leq \frac{\sin \alpha}{\alpha} \leq 1$. Lorsque α tend vers 0^+ , le théorème d'encadrement montre $\lim_{\alpha \rightarrow 0^+} \frac{\sin \alpha}{\alpha} = 1$ car $\lim_{\alpha \rightarrow 0^+} \cos \alpha = 1$. Vu que $\frac{\sin(-\alpha)}{-\alpha} = \frac{\sin \alpha}{\alpha}$, le résultat reste vrai en 0^- . \square

Remarque. Ceci prouve au passage que la fonction sinus est dérivable en 0.

Lemme. On a $\lim_{\alpha \rightarrow 0} \frac{\cos \alpha - 1}{\alpha} = 0$.

Preuve. On a vu pour $\alpha > 0$ que $1 - \frac{\alpha^2}{2} \leq \cos \alpha \leq 1$ (formule qui reste inchangée si $\alpha < 0$). Il suit $-\frac{\alpha}{2} \leq \frac{\cos \alpha - 1}{\alpha} \leq 0$ et le théorème d'encadrement montre la limite nulle. Même méthode avec $\alpha < 0$, ce qui permet d'obtenir le résultat souhaité. \square

Remarque. Ceci prouve au passage que la fonction cosinus est dérivable en 0.

5.2.2 Dérivées du sinus et du cosinus

Théorème. La fonction sin est dérivable sur \mathbb{R} et sa dérivée est la fonction cos.

Preuve. Soit $x \in \mathbb{R}$; on écrit le taux d'accroissement du sinus en x : $\frac{\sin(x+h) - \sin x}{h} = \frac{\sin x \cos h + \sin h \cos x - \sin x}{h} = \sin x \frac{\cos h - 1}{h} + \cos x \frac{\sin h}{h}$. Nos résultats précédents montrent alors que la limite de ce taux lorsque h tend vers 0 vaut $\sin x \cdot 0 + \cos x \cdot 1 = \cos x$. \square

Théorème. La fonction cos est dérivable sur \mathbb{R} et sa dérivée est la fonction $-\sin$.

Preuve. Il suffit de noter que $\cos x = \sin\left(\frac{\pi}{2} - x\right)$. Le théorème de dérivation d'une fonction composée montre que cos est dérivable et que $\cos' x = -\cos\left(\frac{\pi}{2} - x\right) = -\sin x$. \square

Théorème. Si u est une fonction dérivable alors $\cos u$ et $\sin u$ sont dérivables, avec :

$$(\cos u)' = -u' \sin u \quad \text{et} \quad (\sin u)' = u' \cos u.$$

Preuve. C'est une application directe du théorème de dérivation d'une composée. \square

5.3 Propriétés

5.3.1 Étude

Théorème.

- La fonction sinus est impaire.
- La fonction cosinus est paire.

Preuve. Il suffit de noter que ces fonctions sont définies sur \mathbb{R} et vérifient $\sin(-x) = -\sin x$ et $\cos(-x) = \cos x$ de par leur définition géométrique. \square

Définition. Une fonction f définie sur \mathbb{R} est T -périodique si $f(x+T) = f(x)$ pour tout $x \in \mathbb{R}$.

Théorème. Les fonctions sinus et cosinus sont 2π -périodiques.

Preuve. Ceci découle de leur construction géométrique. \square

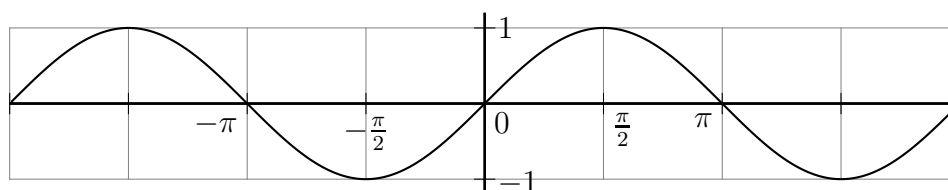
Remarque. Initialement nous devons étudier \sin et \cos sur \mathbb{R} . Leur périodicité permet de ramener l'étude à l'intervalle (de la mesure principale) $] -\pi; \pi]$, puis leur parité permet de se contenter de $[0; \pi[$. Sur cet intervalle réduit, on obtient facilement :

x	0	$\frac{\pi}{2}$	π
$\cos x$	+	0	-
$\sin x$	0	1	0

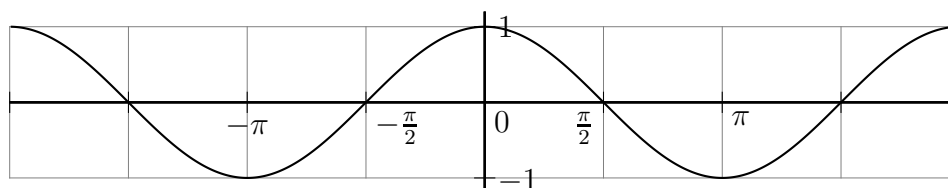
x	0	$\frac{\pi}{2}$	π
$-\sin x$	-	0	-
$\cos x$	1	0	-1

5.3.2 Courbes

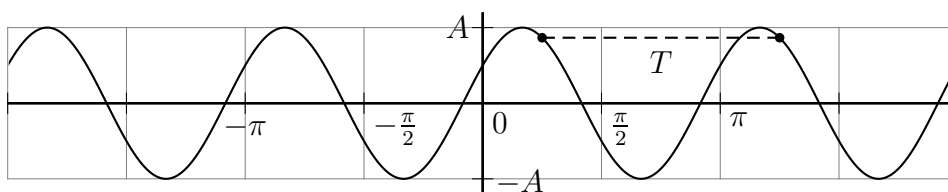
Sinus



Cosinus



Sinusoïde $A \sin(\omega t + \varphi)$



Ici A est l'*amplitude*, ω la *pulsation* (i.e. vitesse angulaire), T la *période* et φ le *déphasage* (décalage temporel horizontal).

On a les relations $\omega = \frac{2\pi}{T} = 2\pi f$, où f est la *fréquence*.

Théorème. Une fonction $f(t) = A \cos \omega t + B \sin \omega t$ est une sinusoïde.

Preuve. Soit $C = \sqrt{A^2 + B^2}$. On a : $f(t) = C \left(\frac{A}{C} \cos \omega t + \frac{B}{C} \sin \omega t \right)$. On note alors que $\left(\frac{A}{C} \right)^2 + \left(\frac{B}{C} \right)^2 = 1$ et donc il existe un angle φ vérifiant $\sin \varphi = \frac{A}{C}$ et $\cos \varphi = \frac{B}{C}$. On voit alors apparaître la formule sommatoire du sinus : $f(t) = C(\sin \varphi \cos \omega t + \cos \varphi \sin \omega t)$ qui donne $f(t) = C \sin(\omega t + \varphi)$. □

5.4 Exercices

Généralités

5.1. Simplifier les expressions $\cos(-x)$, $\sin(-x)$, $\cos(x + \pi)$, $\sin(x + \pi)$, $\cos(\pi - x)$, $\sin(\pi - x)$, $\cos\left(x + \frac{\pi}{2}\right)$, $\sin\left(x + \frac{\pi}{2}\right)$, $\cos\left(\frac{\pi}{2} - x\right)$ et $\sin\left(\frac{\pi}{2} - x\right)$.

5.2. 1. Quelle est la période de la sinusoïde $5 \cos(3t + 4)$?

2. Quelle est la période de la fonction $\sin(6t + 1) + \sin(9t - 5)$?

Limites

5.3. Montrer que la fonction sinus ne converge pas en $+\infty$.

5.4. Calculer la limite de $\frac{\sin ax}{\sin bx}$ ($a, b \neq 0$) lorsque x tend vers 0.

5.5. Calculer la limite de $\frac{\cos x}{x - \frac{\pi}{2}}$ lorsque x tend vers $\frac{\pi}{2}$.

5.6. Calculer la limite de $\frac{\sin x}{x}$ lorsque x tend vers $+\infty$.

5.7. Calculer la limite de $x + \sin x$ lorsque x tend vers $+\infty$.

5.8. Calculer la limite de $\frac{x + \sin x}{\sqrt{x} - 1}$ lorsque x tend vers $+\infty$.

Dérivation

5.9. Montrer que, si x est petit, $\sin\left(\frac{\pi}{6} + x\right) \approx \frac{1}{2} + \frac{\sqrt{3}}{2}x$. En déduire une approximation de $\sin\left(\frac{\pi}{6} + \frac{\pi}{666}\right)$ sans utiliser les fonctions trigonométriques.

5.10. Montrer que la fonction f définie sur \mathbb{R} par $f(x) = x^2 \sin \frac{1}{x}$ si $x \neq 0$ et $f(0) = 0$ est dérivable en 0 et calculer son nombre dérivé.

5.11. Calculer les dérivées des fonctions suivantes :

1. $\sin 2x$;

2. $3x \sin x$;

3. $\sin \frac{1}{x}$;

4. $\cos^3 x$.

5.12. Soit $x(t) = A \sin(\omega t + \varphi)$. Vérifier que $x'' + \omega^2 x = 0$ (équation différentielle linéaire du second ordre d'un oscillateur libre).

5.13. Quelle est le meilleur angle que doivent former les deux trous d'une lunule faite avec une broche à glace ?

Étude de la fonction tangente

5.14. On définit la *fonction tangente* par la formule $\tan x = \frac{\sin x}{\cos x}$.

1. Déterminer son ensemble de définition.
2. Montrer que \tan est impaire et π -périodique. En déduire un intervalle d'étude I pertinent.
3. Déterminer les limites de \tan sur I et ses asymptotes.
4. Montrer que \tan est dérivable sur son ensemble de définition puis établir deux expressions de sa dérivée.
5. Déterminer les variations de \tan sur I ainsi que sa dérivée en 0.
6. Tracer rapidement \tan sur $\left]-\frac{\pi}{2}; \frac{3\pi}{2}\right[$.

Études de fonctions

5.15. Étudier la fonction $\frac{\sin x}{2 + \cos x}$ sur \mathbb{R} .

5.16. Montrer que l'équation $\tan x = x$ possède une unique solution dans $\left]\frac{\pi}{2}; \frac{3\pi}{2}\right[$.

5.17. Soit $P(x) = 2x^3 + x^2 - 5x + 2$.

1. Trouver une racine évidente de P puis le factoriser.
2. Établir le tableau de signe de P .
3. Résoudre sur $]-\pi; \pi]$ l'inéquation $2\cos^3 x + \cos^2 x - 5\cos x + 2 \leq 0$.

5.18. Soit f la fonction définie sur $\left[0; \frac{\pi}{2}\right[$ par $f(x) = 2\sin x + \tan x - 3x$.

1. Montrer que $f'(x)$ est du même signe que $2\cos^3 x - 3\cos^2 x + 1$.
2. Soit $P(X) = 2X^3 - 3X^2 + 1$. Étudier le signe de $P(X)$ lorsque $X \in]0; 1]$.
3. En déduire les variations de f .
4. Montrer que $2\sin x + \tan x \geq 3x$ pour tout $x \in \left[0; \frac{\pi}{2}\right[$.

5.19. 1. Montrer que l'équation $\cos x = x$ possède une unique solution α dans \mathbb{R} .

2. Trouver graphiquement le maximum M de $\left|\frac{\cos x - \cos \alpha}{x - \alpha}\right|$ lorsque $0 \leq x \leq 1$.
3. Étudier avec un tableur et avec un algorithme de tracé la suite (u_n) définie par $u_0 = 0$ et $u_{n+1} = \cos u_n$.
4. Montrer par récurrence que $0 \leq u_n \leq 1$.
5. Montrer que (u_n) converge vers α en établissant d'abord que $|u_{n+1} - \alpha| \leq M|u_n - \alpha|$.

6. Exponentielle

6.1 Construction et propriétés élémentaires

6.1.1 Existence et unicité

Théorème. Soit k un réel non nul. Il existe une unique fonction f , dérivable sur \mathbb{R} , qui vérifie le *problème de Cauchy* (i.e. une équation différentielle avec conditions initiales) :

$$(S) \begin{cases} f' = kf \\ f(0) = 1 \end{cases}$$

Preuve. • *Existence.* L'idée sera montrée à la section 6.4, en utilisant la méthode d'Euler.

- *Unicité.* Soient f et g vérifiant (S) et soit $\varphi(x) = f(x)g(-x)$. Cette fonction produit est dérivable sur \mathbb{R} et $\varphi'(x) = f'(x)g(-x) + f(x)(-g'(-x)) = k\varphi(x) - k\varphi(x) = 0$. Ainsi φ est constante sur \mathbb{R} avec $\varphi(x) = \varphi(0) = f(0)g(0) = 1$ pour tout réel x . On obtient donc en particulier $g(x)g(-x) = 1$ i.e. $g(x) = \frac{1}{g(-x)}$. Finalement $f(x) = \frac{1}{g(-x)} = g(x)$ pour tout réel x , i.e. $f = g$.

□

Définition. Dans le cas général les solutions sont appelées *fonctions exponentielles*. Si $k = 1$, la solution est appelée *exponentielle*, notée \exp . On a donc

$$\begin{cases} \exp' = \exp \\ \exp(0) = 1 \end{cases}$$

6.1.2 Propriétés élémentaires

Théorème. Quel que soit le réel x , $\exp(-x) = \frac{1}{\exp(x)}$.

Preuve. Déjà vue lors de la démonstration de l'unicité.

□

Théorème. • Quel que soit le réel x , $\exp(x) > 0$;
• \exp est strictement croissante sur \mathbb{R} .

Preuve. Le deuxième point résulte clairement du premier puisque $\exp' = \exp$. On a vu que $\exp(x)\exp(-x) = 1$, donc la fonction \exp ne s'annule jamais. On sait de plus que $\exp(0) = 1 > 0$; si \exp possédait une valeur négative, le théorème des valeurs intermédiaires montrerait l'existence d'une racine, ce qui est impossible.

□

6.2 Propriétés algébriques et notation exponentielle

6.2.1 Propriétés de puissance

Théorème (fondamental). Quels que soient les réels x et y , $\exp(x + y) = \exp(x) \exp(y)$.

Preuve. On pose $\varphi(x) = \exp(x + y) \exp(-x) \exp(-y)$. Cette fonction produit est dérivable et $\varphi'(x) = \exp(x + y) \exp(-x) \exp(-y) + \exp(x + y)(-\exp(-x)) \exp(-y) = 0$. Ainsi φ est constante, égale à $\varphi(0) = 1$. Finalement $\exp(x + y) \exp(-x) \exp(-y) = 1$, soit $\exp(x + y) = \exp(x) \exp(y)$. \square

Remarque. L'exponentielle (comme toutes les fonctions exponentielles) transforme donc une somme en produit.

Corollaire. Soient $x, y \in \mathbb{R}$. On a :

- $\exp(x - y) = \frac{\exp(x)}{\exp(y)}$;
- $\exp(nx) = \exp(x)^n$ où $n \in \mathbb{Z}$;
- $\exp\left(\frac{x}{n}\right) = \sqrt[n]{\exp(x)}$ où $n \in \mathbb{N}^*$.

Preuve. • On écrit $\exp(x - y) = \exp(x + (-y)) = \exp(x) \exp(-y) = \frac{\exp(x)}{\exp(y)}$.
 • On procède par récurrence sur $n \in \mathbb{N}$. Initialisation : on a trivialement $\exp(0) = \exp(x)^0$.
 Hérédité : $\exp((n + 1)x) = \exp(nx + x) = \exp(nx) \exp(x) = \exp(x)^n \exp(x) = \exp(x)^{n+1}$.
 On étend facilement ce résultat à $n \in \mathbb{Z}$.
 • On utilise la propriété précédente : $\exp\left(\frac{x}{n}\right)^n = \exp\left(n \frac{x}{n}\right) = \exp(x)$. \square

6.2.2 Notation exponentielle

Définition. La *base* de l'exponentielle est le nombre $e = \exp(1) \approx 2,718$.

Remarque. • Si n est un entier, alors $\exp(n) = \exp(n \times 1) = \exp(1)^n = e^n$.
 • Si $\frac{p}{q} \in \mathbb{Q}$, on calcule $\exp\left(\frac{p}{q}\right)^q = \exp\left(q \frac{p}{q}\right) = \exp(p) = e^p$. Par définition de la racine q -ième, on a $\exp\left(\frac{p}{q}\right) = (e^p)^{\frac{1}{q}} = e^{\frac{p}{q}}$.
 • Les propriétés algébriques de l'exponentielle sont celles des puissances.

Définition. On est donc amené à noter par extension $e^x = \exp(x)$ pour $x \in \mathbb{R}$.

Remarque. Les règles algébriques sont celles des puissances entières. (Au chapitre 8 nous verrons en quoi e^x est *vraiment* une puissance.) Lorsqu'on écrit e^r où r est un rationnel, la précédente remarque prouve qu'il n'y a aucune ambiguïté quant aux modes de calcul (exponentielle ou puissance « classique »), puisqu'ils coïncident sur \mathbb{Q} .

6.2.3 Équation fonctionnelle

Nous savons déjà qu'une fonction exponentielle transforme une somme en produit. Ce sont en fait les seules fonctions ayant cette propriété :

Théorème. Soit f une fonction dérivable sur \mathbb{R} ne s'annulant pas et transformant une somme en produit, i.e. $f(x+y) = f(x)f(y)$. Alors f est une fonction exponentielle.

Preuve. On a $f(0+0) = f(0)f(0)$ donc $f(0) = 1$ car $f(0) \neq 0$. Ensuite, posons $\varphi(x) = f(x+y) - f(x)f(y)$. On a évidemment $\varphi(x) = 0$. Cette fonction est dérivable, et $\varphi'(x) = f'(x+y) - f'(x)f(y) = 0$ puisque $\varphi = 0$. En prenant $x = 0$, il vient $f'(y) = f'(0)f(y)$. En notant $k = f'(0)$, on arrive bien à $f'(y) = kf(y)$ et $f(0) = 1$. \square

Définition. L'équation $f(x+y) = f(x)f(y)$ est appelée *relation fonctionnelle caractéristique* de l'exponentielle.

6.3 Propriétés analytiques

6.3.1 Approximation à l'origine et inégalité fondamentale

Théorème. La tangente en 0 à la courbe de l'exponentielle est d'équation $y = x + 1$.

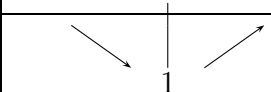
Preuve. L'équation de cette tangente est $y - e^0 = \exp'(0)(x - 0)$, soit $y - 1 = e^0 x$, ce qui donne $y = x + 1$. \square

Théorème. L'approximation affine en 0 de l'exponentielle est $e^x \approx 1 + x$.

Preuve. C'est une autre forme de l'équation de la tangente en 0... \square

Théorème. Quel que soit $x \in \mathbb{R}$, $e^x > x$.

Preuve. Soit $\varphi(x) = e^x - x$. Cette fonction est dérivable, et $\varphi'(x) = e^x - 1$. Puisque l'exponentielle est croissante, φ' l'est aussi, et on obtient le tableau de variation suivant :

x	$-\infty$	0	$+\infty$
$\varphi'(x)$	-	0	+
$\varphi(x)$			

Ainsi $\varphi(x) \geq 1$ d'où $e^x \geq 1 + x$ (la tangente en 0) et finalement $e^x > x$. \square

6.3.2 Comportement asymptotique

Théorème. • $\lim_{x \rightarrow +\infty} e^x = +\infty$;

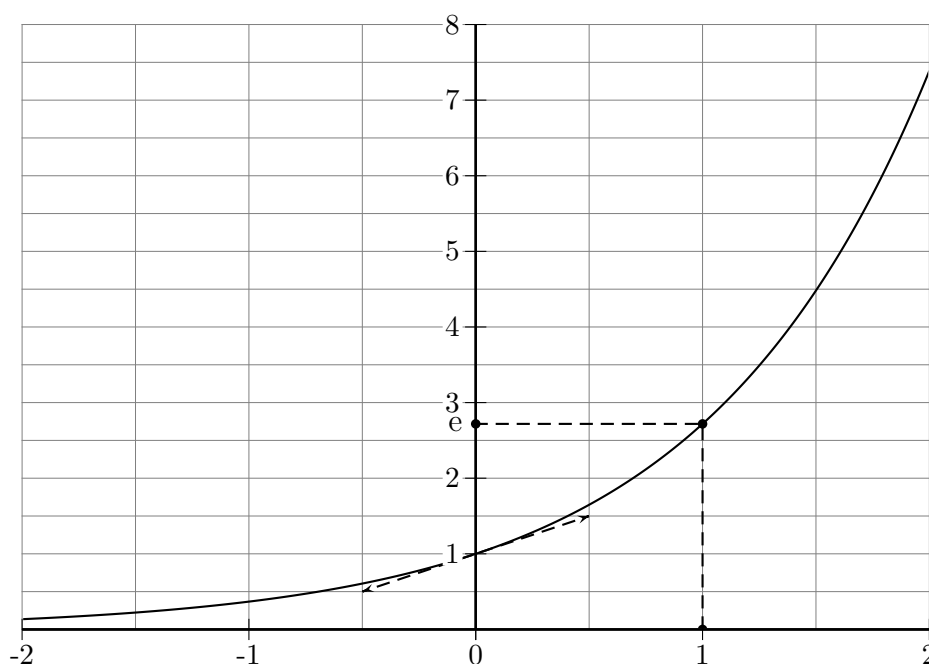
- $\lim_{x \rightarrow -\infty} e^x = 0$;
- $\lim_{x \rightarrow +\infty} \frac{x^n}{e^x} = \lim_{x \rightarrow -\infty} x^n e^x = 0$;
- $\lim_{x \rightarrow +\infty} \frac{P(x)}{e^x} = \lim_{x \rightarrow -\infty} P(x) e^x = 0$ où P est une fonction polynôme.

Preuve. • On a $e^x \geq x$; la limite suit, par le théorème de minoration.

- On remarque que $\lim_{x \rightarrow -\infty} e^x = \lim_{x \rightarrow +\infty} e^{-x} = \lim_{x \rightarrow +\infty} \frac{1}{e^x} = 0$ par ce qui précède.
- L'astuce est d'observer que $\left(e^{\frac{x}{n+1}}\right)^{n+1} \geq \left(\frac{x}{n+1}\right)^{n+1}$ donne $e^x \geq \frac{x^{n+1}}{(n+1)^{n+1}}$. Ainsi $\frac{x^n}{e^x} \leq \frac{(n+1)^{n+1}}{x}$ et la limite recherchée est donc nulle par majoration.
- On factorise le polynôme par son terme de plus haut degré puis on utilise le résultat précédent.

□

6.3.3 Courbe représentative



6.4 Construction de l'exponentielle

On considère l'équation différentielle censée définir l'exponentielle : $y' = y$ et $y(0) = 1$.
On va montrer les idées qui conduisent aux résultats suivants :

- la méthode d'Euler fournit une suite d'approximation ;
- cette suite converge vers une fonction y ;
- cette fonction y est dérivable et vérifie bien $y' = y$.

6.4.1 Méthode d'Euler

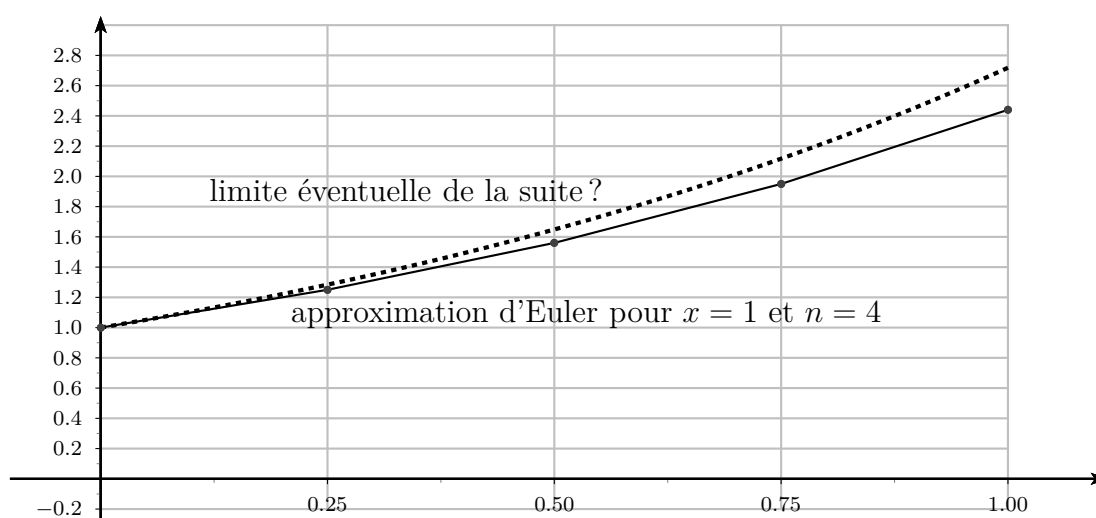
L'idée de la méthode d'Euler est d'utiliser des successions d'approximations différentielles affines pour approcher la courbe \mathcal{C} de la fonction y .

On se donne un $x > 0$ et on découpe l'intervalle $[0; x]$ en n parties égales, donc de largeur $h = \frac{x}{n}$.

On pose $y_0 = y(0) = 1$. En partant du point originel $(0; 1)$, on peut estimer que l'ordonnée du point d'abscisse h de la courbe \mathcal{C} vaut $y(h) \approx y_1 = 1 + y'(0) \cdot h = 1 + y(0) \cdot h = 1 + h$.

De manière générale, on peut estimer $y((k+1)h) \approx y_{k+1} = y_k + y'(kh) \cdot h = y_k + y(kh) \cdot h \approx y_k + y_k \cdot h = (1+h)y_k$. (On notera que l'on commet ici deux erreurs : une sur le point de départ y_k et l'autre sur l'approximation affine.)

La suite (y_k) est donc géométrique de raison $(1+h)$ et ainsi $y_k = y_0(1+h)^k = (1+h)^k$. Lorsque l'on arrive en $x = nh$, il vient $y(x) \approx y_n = (1+h)^n = \left(1 + \frac{x}{n}\right)^n$.



6.4.2 Existence

Théorème.

- Pour tout x , la suite d'approximation d'Euler $\left(1 + \frac{x}{n}\right)^n$ converge vers un réel noté $\exp(x)$;
- la fonction \exp ainsi obtenue est dérivable et sa dérivée est \exp .

Preuve (idée). On définit $u_n(x) = \left(1 + \frac{x}{n}\right)^n$ et $v_n(x) = \left(1 - \frac{x}{n}\right)^{-n}$. L'idée est ici qu'en supposant \exp construite et n grand, $\left(1 + \frac{x}{n}\right)^n \approx e^x$ et $\left(1 - \frac{x}{n}\right)^{-n} \approx (e^{-x})^{-1} = e^x$. On peut montrer ensuite, assez difficilement, que ces deux suites sont adjacentes pour $n > |x|$ et donc convergent. On prouve que la limite obtenue est dérivable en calculant son taux de variation. L'inégalité-clé de toute la preuve est $(1+x)^n \geq 1+nx$ pour $x \geq -1$ (Bernoulli), que nous avons déjà montrée par récurrence. \square

6.5 Exercices

Généralités

- 6.1.** Montrer que $e^x = e^y \Leftrightarrow x = y$ et que $e^x < e^y \Leftrightarrow x < y$.
- 6.2.** Montrer que l'exponentielle réalise une bijection de \mathbb{R} sur \mathbb{R}_+^* .
- 6.3.** Montrer que si u est dérivable, alors $(e^u)' = u'e^u$.

Manipulations algébriques

- 6.4.** Simplifier les écritures des expressions suivantes :

1. $e^x e^{-x}$;
2. ee^x ;
3. $\frac{(e^x)^3}{e^{2-x}}$.

- 6.5.** Vérifier les égalités suivantes :

1. $(e^x + e^{-x})^2 = e^{2x} + \frac{1}{e^{2x}} + 2$;
2. $(e^x + e^{-x})^2 - (e^x - e^{-x})^2 = 4$;
3. $e^{2x} + 1 = e^x(e^x + e^{-x})$;
4. $\frac{1}{1 + e^{-x}} = \frac{e^x}{e^x + 1}$.

- 6.6.** Montrer que la fonction f , définie sur \mathbb{R} par $f(x) = \frac{e^x - 1}{e^x + 1}$, est impaire.

- 6.7.** Soit P un polynôme et f la fonction définie sur \mathbb{R} par $f(x) = P(x)e^x$. Montrer que f est dérivable et que $f'(x) = Q(x)e^x$, où Q est un polynôme de même degré que P .

Résolutions d'équations et d'inéquations

- 6.8.** Résoudre les équations suivantes :

1. $e^{2x} - e = 0$;
2. $e^{x-1} = e^{2-3x}$;
3. $e^{2x+1} - (e^x)^3 = 0$;
4. $\exp\left(1789 \arctan(x\sqrt{1515})\right) + \exp\left(-1492x + \sqrt[52]{|x|}\right) = 0$;
5. $e^x - 5e^{-x} + 4 = 0$ avec $x > 0$;
6. $e^{2x} + 2e^x - 3 = 0$.

- 6.9.** Résoudre les inéquations suivantes :

1. $2xe^{-2x} - e^{-2x} > 0$;
2. $e^{x-x^2} \geq 1$;
3. $3e^{2x} + e^x - 4 \geq 0$;
4. $e^x - 2e^{-x} + 1 \geq 0$.

Calculs de limites

6.10. Calculer les limites des fonctions suivantes :

1. $e^x - x$ en $+\infty$;
2. $e^x - x^{17}$ en $+\infty$ (à tracer d'abord sur un grapheur) ;
3. $(x^2 - 3x)e^x$ en $-\infty$;
4. $\frac{xe^x}{x + e^x}$ en $+\infty$;
5. $\exp \frac{1}{x^2}$ en $-\infty$;
6. $e^{-3x}\sqrt{x^2 + 1}$ en $+\infty$;
7. $\frac{e^{2x} - 1}{x}$ en 0 ;
8. $\frac{e^{2x} - e^x}{x}$ en 0 ;
9. $x \exp \frac{1}{x}$ en 0 ;
10. $xe^{\sin x}$ en $+\infty$.

Études de fonctions

6.11. On définit sur \mathbb{R} les fonctions :

$$\begin{cases} \operatorname{ch}(x) &= \frac{e^x + e^{-x}}{2} & (\text{cosinus hyperbolique}) \\ \operatorname{sh}(x) &= \frac{e^x - e^{-x}}{2} & (\text{sinus hyperbolique}) \end{cases}$$

1. Montrer que $\operatorname{ch}^2 x - \operatorname{sh}^2 x = 1$.
Ceci justifie l'adjectif « hyperbolique », en lien avec l'hyperbole d'équation $X^2 - Y^2 = 1$.
2. Montrer que ces deux fonctions sont dérivables puis calculer leurs dérivées.
3. Étudier la parité de ch et sh .
4. Étudier les variations de ch et sh .
5. Calculer les limites de ch et sh en $\pm\infty$.
6. Déterminer les tangentes de ch et sh en $x = 0$.
7. Montrer que ch et sh sont asymptotes en $+\infty$.

6.12. Soit f la fonction définie sur \mathbb{R} par $f(t) = \frac{10}{1 + \exp(2 - 0,5t)}$.

1. Déterminer les limites de f .
2. Déterminer le sens de variation de f .
3. Montrer que la courbe de f admet le point $\Omega(4; 5)$ comme centre de symétrie.
4. Montrer que f satisfait l'équation différentielle $f'(t) = \frac{1}{20}f(t)(10 - f(t))$.

6.13. Soit f la fonction définie sur \mathbb{R} par $f(x) = x + 1 - xe^{-x^2+1}$.

1. Montrer que $f'(x) = 1 + (2x^2 - 1)e^{-x^2+1}$ puis que f' est paire.
2. Établir le tableau de variation de f' .
3. Montrer que f' possède une unique racine α sur \mathbb{R}_+ , comprise entre 0,51 et 0,52.
4. Étudier les variations de f .
5. Exprimer $f(\alpha)$ sous la forme d'une fraction rationnelle en α .

6.14. La densité de probabilité de présence radiale de l'électron d'un atome d'hydrogène à l'état fondamental est donnée par $d(r) = 4a_0^{-3}r^2e^{-2r/a_0}$ où $a_0 \approx 5,291772 \cdot 10^{-11}\text{m}$ est le *rayon de Bohr*. Montrer que cette densité atteint un maximum en un rayon r que l'on précisera.

Modèles d'évolution

6.15. 1. Montrer que les solutions de $y' = ay$ sont exactement les fonctions $y(x) = Ce^{ax}$ où C est une constante.

2. Montrer, en se ramenant par un changement de variable au cas précédent, que les solutions de $y' = ay + b$ sont exactement les fonctions $y(x) = Ce^{ax} - \frac{b}{a}$ où C est une constante.

6.16 (radioactivité). On rappelle que si $N(t)$ est le nombre de noyaux d'un corps radioactif à l'instant t , la vitesse de variation $\frac{\Delta N(t)}{\Delta t}$ de ce nombre (par désintégration) est proportionnelle à $N(t)$.

1. Supposons que N soit dérivable (est-ce d'ailleurs possible?). Montrer qu'il existe $\lambda > 0$ tel que $N'(t) = -\lambda N(t)$.
2. Résoudre cette équation.
3. Le *temps caractéristique* est le nombre $\tau = \frac{1}{\lambda}$. Exprimer la demi-vie en fonction de τ .

6.17 (datation au carbone 14). Le carbone 14 est un isotope instable du carbone 12. On admet qu'il se trouve en proportion constante dans les organismes vivants qui absorbent du carbone. Cette proportion P_0 de noyaux de C_{14} par rapport aux noyaux de C_{12} est voisine de $1,3 \cdot 10^{-10}\%$. Quand un organisme meurt, il n'absorbe plus de C_{14} et celui-ci se désintègre en azote. En physique, on montre que le rapport $P(t)$ de la quantité de C_{14} sur celle de C_{12} vérifie $\frac{P'(t)}{P(t)} = -1,21 \cdot 10^{-4}$.

1. Sur quel intervalle I la fonction P est-elle définie? Déterminer la fonction P .
2. Étudier les variations de P sur I .
3. Démontrer qu'il existe un nombre t_0 , appelé *demi-vie*, tel que $P(t_0) = \frac{1}{2}P_0$.
4. L'analyse d'un fragment d'os a révélé une proportion de $0,2 \cdot 10^{-10}\%$ de C_{14} . Peut-on penser que ce fragment d'os date de plus de 10000 ans?

6.18 (thermodynamique). La variation de température (en $^{\circ}\text{C}$) d'un matériau est proportionnelle à la différence entre sa température et la température extérieure.

1. Montrer que $\frac{dT}{dt} = -k(T - T_{ext})$ où k est une constante positive.
2. On suppose que la température extérieure est de 30°C et qu'à $t = 0$ le matériau est à 100°C . Montrer que $T = 30 + 70e^{-kt}$.

6.19 (charge d'un condensateur). On considère un montage en série d'un condensateur C et d'une résistance R , soumis à une tension constante E à partir de $t = 0$. On pose $\tau = RC$ (*temps caractéristique*).

1. Montrer que la quantité de courant $q(t)$ vérifie l'équation $\frac{dq}{dt} = -\frac{1}{RC}q + \frac{E}{R}$.
2. En déduire l'expression de $q(t)$ puis de la tension $u_C(t)$.
3. Montrer que la limite de $u_C(t)$ lorsque t tend vers l'infini vaut E . Quelle est alors la situation dans le circuit ?
4. On suppose que l'on a obtenu la courbe de charge sur une durée suffisante à sa stabilisation en E . On considère qu'un condensateur est chargé lorsque u_C vaut 99% de E . Les physiciens, qui aiment les choses pratiques, prétendent que l'on peut alors trouver τ de l'une des manières suivantes :
 - le condensateur est chargé lorsque $t = 4,6\tau$;
 - lorsque $t = \tau$, la tension u_C vaut 63% de E ;
 - τ est l'abscisse de l'intersection de la tangente à l'origine avec la droite horizontale d'ordonnée E .

Peut-on leur donner raison ? Ces méthodes vous paraissent-elles toutes fiables ?

6.20 (loi logistique continue). Pour certaines populations vivant dans un milieu clos (bactéries dans une coupelle de culture par exemple), la croissance est dans un premier temps exponentielle, mais ensuite freinée par surpopulation (manque de nourriture, d'oxygène, etc...). Le mathématicien P. Verhulst a proposé vers 1840 le modèle suivant.

La population ne peut dépasser un seuil critique, et on note $y(t)$ la fraction de la population à l'instant t sur cette population maximale. L'équation $y' = \lambda y(1 - y)$ est alors supposée vérifiée, et est appelée *équation logistique continue* (à rapprocher de sa version discrète déjà étudiée).

1. Vérifier que, dans un premier temps, la croissance est à peu près exponentielle.
2. Résoudre cette équation, en posant $z = \frac{1}{y}$.
3. Si $y(0) = 0,01$ et $\lambda = 1$, exprimer $y(t)$ en fonction de t , puis tracer la courbe de y .

7. Nombres complexes

7.1 Généralités

En 1545, l'Italien Cardan publie *Ars Magna*, dans lequel il cherche entre autre à résoudre l'équation $x^2 + 40 = 10x$. Il trouve deux solutions, $5 \pm \sqrt{-15}$, qu'il juge *vraiment imaginaires*. L'école italienne suit alors cette voie au 16ème siècle. Beaucoup plus tard, en 1777, Euler pose $i = \sqrt{-1}$, notation popularisée ensuite par Gauss en 1801.

Théorème.

- Il existe un symbole, noté i , vérifiant $i^2 = -1$.
- Il existe un ensemble de nombres, le *corps des nombres complexes*, noté \mathbb{C}
 - prolongeant le corps des nombres réels (nombres et opérations) ;
 - tel que tout *nombre complexe* s'écrive $a + ib$ où a et b sont des réels.

Preuve. Admise ; une construction simple mais très laborieuse est possible au lycée en identifiant \mathbb{C} avec \mathbb{R}^2 (les couples de réels). □

Remarque.

- L'*inclusion naturelle* de \mathbb{R} dans \mathbb{C} est définie en écrivant un réel x sous la forme $x + i0$.
- Les opérations sur les nombres complexes sont ainsi très naturelles, en considérant i comme un réel ayant la particularité de valoir -1 lorsqu'il est élevé au carré.

Théorème. L'écriture d'un nombre complexe est unique.

Preuve. Soit $z = x + iy \in \mathbb{C}$. Si z est nul, alors $x + iy = 0$ donne $x = -iy$. Ainsi $x^2 = -y^2$, ce qui implique $x = y = 0$. Prenons maintenant deux complexes égaux $x + iy = x' + iy'$. On obtient $(x - x') + i(y - y') = 0$ et donc $x - x' = 0$ et $y - y' = 0$, i.e. $x = x'$ et $y = y'$. □

Définition.

- Si $z = a + ib$, alors $a = \operatorname{Re}(z)$ est sa *partie réelle* et $b = \operatorname{Im}(z)$ est sa *partie imaginaire*.
- Si $\operatorname{Im}(z) = 0$, i.e. $z = a$, alors z est *réel*.
- Si $\operatorname{Re}(z) = 0$, i.e. $z = ib$, alors z est *imaginaire pur*.
- L'écriture $z = a + ib$ est la *forme algébrique (ou cartésienne)* de z .

7.2 Conjugué et module

7.2.1 Conjugué

Définition. Si $z = x + iy$ alors $\bar{z} = x - iy$ est le *conjugué* de z .

Théorème.

- $z = \bar{z} \Leftrightarrow \operatorname{Im}(z) = 0 \Leftrightarrow z$ réel ;
- $z = -\bar{z} \Leftrightarrow \operatorname{Re}(z) = 0 \Leftrightarrow z$ imaginaire pur ;
- $\overline{\bar{z}} = z$;

- $\overline{z + z'} = \overline{z} + \overline{z'}$;
- $\overline{zz'} = \overline{z}\overline{z'}$;
- $\overline{\left(\frac{1}{z}\right)} = \frac{1}{\overline{z}}$;
- $\overline{\left(\frac{z}{z'}\right)} = \frac{\overline{z}}{\overline{z'}}$.

Preuve. Simples calculs, en revenant à la définition. □

Théorème (formules d'Euler). On a $\operatorname{Re}(z) = \frac{z + \overline{z}}{2}$ et $\operatorname{Im}(z) = \frac{z - \overline{z}}{2i}$.

Preuve. Il suffit de revenir à la définition de \overline{z} : $z + \overline{z} = 2x$ et $z - \overline{z} = 2iy$. □

7.2.2 Module

Définition. Si $z = x + iy$, le *module* de z est le réel positif $|z| = \sqrt{x^2 + y^2}$.

Théorème. • Le module dans \mathbb{C} prolonge la valeur absolue de \mathbb{R} , i.e. $|x + i0|_{\mathbb{C}} = |x|_{\mathbb{R}}$.

- $|z| = 0 \Leftrightarrow z = 0$.
- $z\overline{z} = |z|^2$.
- $|\overline{z}| = |z|$.
- $|zz'| = |z||z'|$.
- $\left|\frac{z}{z'}\right| = \frac{|z|}{|z'|}$.
- $\frac{1}{z} = \frac{\overline{z}}{|z|^2}$.

Preuve. Les deux premiers résultats sont évidents. Le point-clé est le troisième ; il se démontre par simple calcul sous forme algébrique. Les autres items s'en déduisent aisément, en considérant les égalités au carré. □

Théorème (inégalité triangulaire). Pour tous complexes z et z' , on a $|z + z'| \leq |z| + |z'|$; l'égalité (hors $z = 0$ ou $z' = 0$) n'a lieu que s'il existe $k \in \mathbb{R}_+$ vérifiant $z' = kz$.

Preuve. D'abord l'inégalité : $|z + z'|^2 = (z + z')\overline{(z + z')} = (z + z')(\overline{z} + \overline{z'}) = z\overline{z} + z\overline{z'} + \overline{z}z' + z'\overline{z'} = |z|^2 + z\overline{z'} + \overline{z}z' + |z'|^2 = |z|^2 + 2\operatorname{Re}(z\overline{z'}) + |z'|^2 \leq |z|^2 + 2|z||z'| + |z'|^2 \leq (|z| + |z'|)^2$.

Ensuite si $z' = kz$ alors $|z + z'| = |(1 + k)z| = (1 + k)|z| = |z| + |z'|$. Réciproquement, s'il y a égalité alors $\operatorname{Re}(z\overline{z'}) = |z||z'|$, et donc $z\overline{z'}$ est un réel k positif. Finalement, $z = k\frac{z'}{|z'|^2}$. □

7.3 Équations du second degré

Remarque. Un réel $a < 0$ possède deux racines carrées complexes imaginaires pures : $i\sqrt{|a|}$ et $-i\sqrt{|a|}$. Ceci nous permet de contourner l'obstacle $\Delta < 0$ lors d'une résolution dans \mathbb{R} . Notons au passage qu'il n'est pas bien vu d'écrire \sqrt{a} si $a < 0$, même si l'on aime l'Italie, du fait que cette notation masque la réalité complexe de ce nombre.

Théorème. L'équation du second degré à coefficients réels $az^2 + bz + c = 0$ avec $\Delta < 0$ possède deux solutions complexes conjuguées $z_1 = \frac{-b + i\sqrt{|\Delta|}}{2a}$ et $z_2 = \frac{-b - i\sqrt{|\Delta|}}{2a}$.

Preuve. Il suffit de reprendre la mise sous forme canonique du cas réel, puis de remarquer que Δ admet $i\sqrt{|\Delta|}$ et $-i\sqrt{|\Delta|}$ comme racines carrées. \square

7.4 Propriétés géométriques

Au 19ème siècle, Gauss, Wessel, Argand et Cauchy commencent à utiliser le plan euclidien pour représenter les nombres complexes.

7.4.1 Plan complexe

Définition. Le *plan complexe* \mathcal{P} est le plan affine euclidien rapporté à un repère orthonormé direct $(0; \vec{u}, \vec{v})$. L'*axe réel* est l'axe des abscisses, et l'*axe imaginaire* est l'axe des ordonnées.

Théorème. La fonction $\varphi : \mathbb{C} \rightarrow \mathcal{P}$ définie par $\varphi(x + iy) = M(x; y)$ est une bijection; elle définit la représentation géométrique naturelle des nombres complexes $M(x + iy) \equiv M(x; y)$.

Preuve. Si l'on se donne $M(x; y)$, on a $\varphi(x + iy) = M$; cet antécédent est de plus unique puisque la forme algébrique d'un complexe l'est. \square

Définition. Soit $z = x + iy$ et soit $M(z)$. Alors :

- z est l'*affixe* de M ;
- z est l'*affixe* de \overrightarrow{OM} ;
- M est l'*image* de z .

Théorème. Les propriétés usuelles des coordonnées sont conservées pour les affixes :

- $|z| = OM$;
- $M'(\bar{z})$ est le symétrique de $M(z)$ par rapport à l'axe réel;
- si $M(z)$ et $M'(z')$ alors $M''(z + z')$ est défini géométriquement par $\overrightarrow{OM''} = \overrightarrow{OM} + \overrightarrow{OM'}$;
- si $M(z)$ et $M'(z')$ alors $\overrightarrow{MM'}(z' - z)$ et $MM' = |z' - z|$.

Preuve. Sans difficulté. \square

7.4.2 Translations et homothéties

Soit $f : \mathcal{P} \rightarrow \mathcal{P}$ avec $f(M) = M'$, $M(z)$ et $M(z')$.

Théorème (translations). $z' = z + b$ où $b \in \mathbb{C}$ est fixé ssi f est la translation de vecteur $\vec{w}(b)$.

Preuve. $z' = z + b$ donne $z' - z = b$ i.e. $\overrightarrow{MM'}(b)$, ce qui caractérise la translation de vecteur $\vec{u}(b)$. \square

Théorème (homothéties). $z' - \omega = k(z - \omega)$ où $\omega \in \mathbb{C}$ et $k \in \mathbb{R}^*$ sont fixés ssi f est l'homothétie de centre $\Omega(\omega)$ et de rapport k .

Preuve. $z' - \omega = k(z - \omega) \Leftrightarrow \overrightarrow{\Omega M'} = k\overrightarrow{\Omega M}$, ce qui caractérise l'homothétie $h(\Omega, k)$. \square

7.4.3 Forme trigonométrique

Il s'agit de la traduction complexe de la forme polaire.

Définition. • Tout complexe non nul z peut s'écrire sous la *forme trigonométrique* (ou *polaire*) $\rho(\cos \theta + i \sin \theta)$ où $\rho = |z|$ et θ est une mesure de $(\vec{u}, \overrightarrow{OM})$ où $M(z)$.

- Le nombre θ est un *argument* de z , noté $\arg z$; le seul argument compris dans $] -\pi; \pi]$ est l'*argument principal*.

Remarque. • Le nombre complexe 0 ne possède pas de forme trigonométrique.

- Si $A(a)$ et $B(b)$, alors $\arg(b - a) = (\vec{u}, \overrightarrow{AB})$ modulo 2π .
- Deux complexes sont égaux ssi ils ont même module et même argument principal.
- Les points du cercle trigonométrique sont ceux d'affixe $\cos \theta + i \sin \theta$.

Théorème. Si $z = x + iy = \rho(\cos \theta + i \sin \theta)$ alors

$$\rho = \sqrt{x^2 + y^2}, \quad \cos \theta = \frac{x}{\rho}, \quad \sin \theta = \frac{y}{\rho}.$$

Preuve. C'est de la trigonométrie de seconde... □

Remarque. • Si θ est remarquable, on l'identifie grâce à son cosinus et son sinus.

- Sinon, on utilise la touche \cos^{-1} (= arccos) d'une calculatrice, qui donne une valeur approchée de $\pm\theta$ modulo 2π . Le signe manquant est ensuite déterminé selon le signe du sinus. Un angle approché est en général exprimé en degrés.
- On peut noter que $\tan \theta = \frac{y}{x}$, ce qui conduit à $\theta = \arctan \frac{y}{x}$ mais malheureusement uniquement modulo π .

7.5 Exponentielle complexe

7.5.1 Définition

Théorème. Soit $f : \mathbb{R} \rightarrow \mathbb{C}$ la fonction définie par $f(\theta) = \cos \theta + i \sin \theta$. Alors

- $f(0) = 1$;
- $f(\theta + \theta') = f(\theta)f(\theta')$.

Preuve. • On calcule $f(0) = 1 + 0i = 1$.

- On a $f(\theta + \theta') = \cos(\theta + \theta') + i \sin(\theta + \theta')$ d'une part, et $f(\theta)f(\theta') = (\cos \theta + i \sin \theta)(\cos \theta' + i \sin \theta') = (\cos \theta \cos \theta' - \sin \theta \sin \theta') + i(\sin \theta \cos \theta' + \cos \theta \sin \theta') = \cos(\theta + \theta') + i \sin(\theta + \theta')$ grâce aux formules trigonométriques sommatoires.

□

Remarque. • Ainsi, f vérifie l'équation fonctionnelle caractéristique des exponentielles, et l'on écrit $f(\theta) = e^{i\theta}$:

$$e^{i\theta} = \cos \theta + i \sin \theta$$

- Toutes les propriétés algébriques des exponentielles sont donc conservées.

- En particulier, $(e^{i\theta})^n = \cos n\theta + i \sin n\theta$, ou encore

$$(\cos \theta + i \sin \theta)^n = \cos n\theta + i \sin n\theta \quad (\text{formule de Moivre}).$$

- Tout complexe non nul peut donc s'écrire $z = \rho e^{i\theta}$ (*forme trigonométrique exponentielle*).

Remarque. On peut retrouver les formules de trigonométrie sommatoires grâce à l'exponentielle complexe, par exemple $\cos(\theta + \theta') = \operatorname{Re}(e^{i(\theta+\theta')}) = \dots = \cos \theta \cos \theta' - \sin \theta \sin \theta'$. On prendra cependant garde au fait que cela n'en fournit pas une preuve, puisqu'on les utilise dans la démonstration du théorème...

7.5.2 Propriétés

Théorème (formules d'Euler). On a $\cos \theta = \frac{e^{i\theta} + e^{-i\theta}}{2}$ et $\sin \theta = \frac{e^{i\theta} - e^{-i\theta}}{2i}$.

Preuve. On note d'une part que $\overline{e^{i\theta}} = \overline{\cos \theta + i \sin \theta} = \cos \theta - i \sin \theta = \cos(-\theta) + i \sin(-\theta) = e^{-i\theta}$ et d'autre part que $\operatorname{Re}(e^{i\theta}) = \cos \theta$ et $\operatorname{Im}(e^{i\theta}) = \sin \theta$. Il suffit ensuite d'appliquer les formules d'Euler générales. \square

Théorème. Soient z et z' deux complexes non nuls. Alors, modulo 2π :

- $\arg(zz') = \arg z + \arg z'$;
- $\arg\left(\frac{z}{z'}\right) = \arg z - \arg z'$;
- $\arg\left(\frac{1}{z}\right) = \arg \bar{z} = -\arg z$;
- $\arg(-z) = \pi + \arg z$;
- $\arg(z^n) = n \arg z$ où $n \in \mathbb{Z}$.

Preuve. Il suffit de mettre d'abord z et z' sous forme exponentielle, puis d'appliquer les propriétés des exponentielles. Par exemple, $\arg\left(\frac{1}{z}\right) = \arg\left(\frac{1}{\rho e^{i\theta}}\right) = \arg\left(\frac{1}{\rho} e^{-i\theta}\right) = -\theta$. Le quatrième point nécessite de noter que $e^{i\pi} = -1$. \square

Remarque. On pourra, au chapitre 8, noter une ressemblance avec les propriétés du logarithme. En mettant de côté (presque) toute rigueur, on constate en effet que $i\theta = \ln e^{i\theta}$. En passant, ceci explique qu'une calculatrice pas trop basique renvoie $\ln(-1) = i\pi$ puisque $-1 = e^{i\pi}$...

Théorème (du quotient). Soient $A(a)$, $B(b)$ et $C(c)$ trois points distincts. Alors le quotient $\frac{c-a}{b-a}$ possède pour module $\frac{AC}{AB}$ et pour argument $(\overrightarrow{AB}, \overrightarrow{AC})$ modulo 2π . En particulier, A , B et C sont alignés ssi $\frac{c-a}{b-a}$ est réel.

Preuve. On calcule d'abord $\left|\frac{c-a}{b-a}\right| = \frac{|c-a|}{|b-a|} = \frac{AC}{AB}$. Ensuite, modulo 2π , $\arg\left(\frac{c-a}{b-a}\right) = \arg(c-a) - \arg(b-a) = (\vec{u}, \overrightarrow{AC}) - (\vec{u}, \overrightarrow{AB}) = (\overrightarrow{AB}, \vec{u}) + (\vec{u}, \overrightarrow{AC}) = (\overrightarrow{AB}, \overrightarrow{AC})$. \square

7.6 Cercles et rotations

Théorème (paramétrisation complexe d'un cercle). Soit $\Omega(\omega)$ un point et soit $\rho > 0$. Alors $M(z)$ appartient au cercle \mathcal{C} de centre Ω et de rayon ρ ssi il existe $\theta \in \mathbb{R}$ tel que $z = \omega + \rho e^{i\theta}$.

Preuve. On procède directement : $M \in \mathcal{C} \Leftrightarrow \Omega M = \rho \Leftrightarrow |z - \omega| = \rho \Leftrightarrow \exists \theta \in \mathbb{R}, z - \omega = \rho e^{i\theta} \Leftrightarrow \exists \theta \in \mathbb{R}, z = \omega + \rho e^{i\theta}$. □

Remarque. Si $\omega = x_\omega + iy_\omega$, on obtient la paramétrisation réelle de \mathcal{C} :

$$M(x; y) \in \mathcal{C} \Leftrightarrow \exists \theta \in \mathbb{R}, \begin{cases} x &= x_\omega + \rho \cos \theta \\ y &= y_\omega + \rho \sin \theta \end{cases}$$

Théorème (caractérisation des rotations). Soit $f : \mathcal{P} \rightarrow \mathcal{P}$, transformant $M(z)$ en $M'(z')$. Alors f est la rotation $r(\Omega, \theta)$ de centre $\Omega(\omega)$ et d'angle θ ssi $z' = \omega + e^{i\theta}(z - \omega)$.

Preuve. Directement, en vertu du théorème du quotient : $f = r(\Omega, \theta) \Leftrightarrow \frac{\Omega M'}{\Omega M} = 1$ et $\left(\overrightarrow{\Omega M}, \overrightarrow{\Omega M'} \right) = \theta \Leftrightarrow \frac{z' - \omega}{z - \omega} = e^{i\theta} \Leftrightarrow z' - \omega = e^{i\theta}(z - \omega)$. □

7.7 Exercices

Forme algébrique

7.1. Soient $z = 1 + 3i$ et $z' = \frac{1}{2} - 2i$.

Calculer sous forme algébrique les nombres $z + z'$, zz' , z^2 , $(z + z')^2$, $\frac{1}{z}$ et $\frac{z'}{z}$.

7.2. Calculer la forme algébrique des nombres suivants :

1. $\frac{1}{4 - 3i}$;
2. $\frac{1 + 2i}{2 - i}$;
3. $\frac{3 + i}{i} + \frac{i}{1 - i\sqrt{2}}$.

7.3. 1. Montrer que la suite (i^n) est périodique.

2. Déterminer i^n en fonction de n .

7.4. L'ensemble des *entiers de Gauss* $\mathbb{Z}[i]$ est composé des nombres complexes dont les parties réelle et imaginaire sont dans \mathbb{Z} . Montrer que le quotient de deux entiers de Gauss appartient à $\mathbb{Q}[i]$.

Équations

7.5. Résoudre dans \mathbb{C} les équations suivantes :

1. $z^2 - 2z + 3 = 0$;
2. $z^2 + \sqrt{2}z + 1 = 0$;
3. $z^4 - z^2 - 12 = 0$;
4. $\frac{1}{z} + z + 1 = 0$;
5. $z + 1 = \frac{3}{2 - z}$.

7.6. Déterminer les nombres complexes z et z' vérifiant $z + z' = 2$ et $zz' = 9$.

7.7. Résoudre l'équation $z^3 + z^2 + z + 1 = 0$.

7.8. 1. Résoudre l'équation $P(z) = z^2 + z + 1 = 0$. On note $j = \frac{-1 + i\sqrt{3}}{2}$.

2. Montrer par réductions successives que $j^3 = 1$.

3. Montrer que $j^2 = \bar{j}$ en prouvant que j^2 est racine de P .

Module, argument et forme trigonométrique

7.9. Montrer que le triangle formé par les points d'affixes 1, j et j^2 est équilatéral.

7.10. Soient u et v deux complexes tels que $|u| = |v| = 1$ et $uv \neq -1$. Montrer que $\frac{u+v}{1+uv}$ est réel. (On se souviendra que $|z|^2 = z\bar{z}$.)

7.11. Placer les complexes $e^{i\frac{\pi}{2}}$, $e^{i\pi}$, $e^{-i\frac{\pi}{2}}$, $e^{i\frac{\pi}{6}}$, $e^{i\frac{\pi}{4}}$, $e^{i\frac{\pi}{3}}$ et $e^{-i\frac{3\pi}{4}}$ sur le cercle trigonométrique.

7.12. Calculer le module et l'argument principal (si possible sous forme exacte) des nombres suivants :

1. $1 + i$;
2. $1 - i$;
3. $\frac{\sqrt{3}}{2} + \frac{1}{2}i$;
4. $1 + 2i$;
5. $-13 - 17i$.

7.13. Calculer la forme algébrique des nombres suivants :

1. $2e^{i\frac{\pi}{3}}$;
2. $\sqrt{2}e^{i\frac{7\pi}{4}}$.

7.14. Calculer la forme trigonométrique exponentielle des nombres suivants :

1. $1, i, -1, -i$;
2. $1 + \sqrt{3}i$;
3. $-1 - i$.

7.15. Calculer la forme algébrique de $(1 + i\sqrt{3})^{2001}$.

7.16. Calculer la forme algébrique de $\left(\frac{1-i}{1+i}\right)^{16}$.

7.17. Soit $z = \frac{1 + i\sqrt{3}}{1 + i}$.

1. Calculer la forme algébrique de z .
2. Calculer la forme trigonométrique de z .
3. En déduire $\cos \frac{\pi}{12}$ et $\sin \frac{\pi}{12}$.

7.18. 1. Soit $\theta \in \left[0; \frac{\pi}{2}\right]$. Déterminer la forme trigonométrique de $1 + e^{i\theta}$. (On pourra factoriser par $e^{i\frac{\theta}{2}}$.).

2. Montrer, dans le cercle trigonométrique, que l'angle au centre est le double de l'angle inscrit.

7.19. Soit $\theta \neq \pi$ (modulo 2π) et soit $t = \tan \frac{\theta}{2}$.

1. Montrer que $\frac{1+it}{1-it} = e^{i\theta}$.
 2. Montrer que $\frac{1+it}{1-it} = \frac{1-t^2}{1+t^2} + i\frac{2t}{1+t^2}$.
 3. En déduire les relations remarquables $\cos \theta = \frac{1-t^2}{1+t^2}$ et $\sin \theta = \frac{2t}{1+t^2}$.
- 7.20.** Soit $n \geq 2$ un entier, et soit, pour $0 \leq k \leq n-1$, $z_k = e^{i\frac{2k\pi}{n}}$.
1. Montrer que les points $M_k(z_k)$ sont les sommets d'un polygone régulier inscrit dans le cercle trigonométrique.
 2. Montrer que $z_k^n = 1$ (z_k est une racine n -ième de l'unité).
 3. Réciproquement, montrer que les solutions de l'équation $z^n = 1$ ont pour images les points M_k .
- 7.21.** Soit $S = 1 + e^{ix} + e^{i2x} + \dots + e^{inx}$ avec $e^{ix} \neq 1$.
1. Montrer que $S = \frac{e^{i(n+1)x} - 1}{e^{ix} - 1}$.
 2. En déduire que $S = e^{i\frac{nx}{2}} \frac{\sin \frac{(n+1)x}{2}}{\sin \frac{x}{2}}$.
 3. Calculer les sommes $1 + \cos x + \cos 2x + \dots + \cos nx$ et $\sin x + \sin 2x + \dots + \sin nx$.
 4. En posant $n = 4$ et $x = \frac{2\pi}{5}$, calculer $\cos \frac{\pi}{5}$ et $\sin \frac{\pi}{5}$.
- 7.22.** Calculer $\cos 3x$ et $\sin 3x$ en fonction de $\cos x$ et $\sin x$ en utilisant la formule de Moivre.
- 7.23.** Montrer que $\cos^3 x = \frac{1}{4} \cos 3x + \frac{3}{4} \cos x$ et $\sin^3 x = -\frac{1}{4} \sin 3x + \frac{3}{4} \sin x$ en utilisant les formules d'Euler (*on a effectué une linéarisation*).

Lieux géométriques

- 7.24.**
1. Déterminer algébriquement (sous forme algébrique) l'ensemble des points $M(z)$ ($z \neq -1$) tels que $\frac{z}{z+1}$ soit réel.
 2. Retrouver géométriquement le résultat en utilisant le théorème du quotient.
- 7.25.**
1. Déterminer algébriquement (sous forme complexe) l'ensemble des points $M(z)$ ($z \neq i$) tels que $\frac{z+i}{z-i}$ soit imaginaire pur.
 2. Retrouver géométriquement le résultat en utilisant le théorème du quotient.
- 7.26.** Déterminer et représenter l'ensemble des points M d'affixe z vérifiant
1. $|z-i| = |z+1|$;
 2. $|z-i+1| = \sqrt{2}$.
- 7.27.** Déterminer et représenter l'ensemble des points M d'affixe z vérifiant
1. $|iz-1| = |z+2-3i|$;
 2. $|1-z| = |\bar{z}|$.
- 7.28.**
1. Montrer que $|z+1|^2 = 2|z|^2$ équivaut à $|z-1|^2 = 2$.
 2. En déduire l'ensemble des points M d'affixe z vérifiant $|z+1| = |\sqrt{2}z|$.

Configurations géométriques

7.29. Soient $A(2)$, $B(-3 + 5i)$, $C(\sqrt{3} + (2 - \sqrt{3})i)$ et $D(6i)$.

1. Montrer que A , B et C sont alignés.
2. Le triangle ABD est-il rectangle ? isocèle ?

7.30. Soient $A(2 + 2i)$, $B\left(\sqrt{3} + \left(\frac{\sqrt{3}}{2} + 1\right)i\right)$, $C\left(-1 + \frac{1}{2}i\right)$ et $D\left(-\frac{1}{4} + \frac{11}{4}i\right)$.

1. Montrer que A , B et C sont alignés.
2. Montrer que D appartient au cercle de diamètre $[AC]$.

7.31. Soient $A(1)$, $B\left(\frac{-1+i}{2}\right)$ et $C\left(\frac{-1-i}{2}\right)$.

1. Montrer que le centre d'inertie du triangle ABC est O .
2. Déterminer le barycentre du système $\{(A, 2), (B, 3), (C, 4)\}$.

7.32. Soient $A(a)$, $B(b)$ et $C(c)$ où $a = -2$, $b = -\frac{1}{5} - \frac{3}{5}i$ et $c = -\frac{1}{5} + \frac{3}{5}i$.

1. Montrer que O , A , B et C sont cocycliques.
2. Soit $D(d)$ où $d = -\frac{1}{2}$. Exprimer sous forme trigonométrique $\frac{a-c}{d-c}$.
3. Que peut-on en déduire ?

7.33. On considère le point A d'affixe $z_A = 2 + i$ et le cercle Γ de centre A et de rayon $\sqrt{2}$.

1. (a) Déterminer les affixes des points d'intersection de Γ avec l'axe réel.
(b) On désigne par B et C les points d'affixes $z_B = 1$ et $z_C = 3$.
Déterminer l'affixe z_D du point D diamétralement opposé au point B sur Γ .
2. Soit M le point d'affixe $\frac{3}{5} + \frac{6}{5}i$.
(a) Calculer $\frac{z_D - z_M}{z_B - z_M}$ et en déduire son argument principal.
(b) Montrer que M appartient au cercle Γ .

7.34. Soient les points $A(1 + i)$, $B(3 - i)$ et $I(2)$.

À tout point $M(z)$ on associe le point $M'(z')$ avec $z' = z^2 - 4z$.

1. Calculer les images A' et B' des points A et B . Que remarque-t-on ?
2. Déterminer les points qui ont pour image le point d'affixe -5 .
3. (a) Vérifier que $z' + 4 = (z - 2)^2$.
(b) En déduire une relation entre $|z' + 4|$ et $|z - 2|$ et, lorsque $z \neq 2$, une relation entre $\arg(z' + 4)$ et $\arg(z - 2)$.
(c) Que peut-on affirmer sur le point M' lorsque M décrit le cercle \mathcal{C} de centre I et de rayon 2 ?
4. Soient les points $E(2 + 2e^{i\frac{\pi}{3}})$, $J(-4)$ et E' l'image de E .
(a) Calculer la distance IE ainsi qu'une mesure de $(\vec{u}, \overrightarrow{IE})$.
(b) Calculer la distance JE' ainsi qu'une mesure de $(\vec{u}, \overrightarrow{JE'})$.
(c) Construire à la règle non graduée et au compas le point E' , en laissant les traits de construction apparents.

Compléments

7.35. Déterminer la forme complexe des transformations suivantes :

1. translation de vecteur $\vec{w}(-1 + i)$;
2. homothétie de centre $\Omega(1 + 3i)$ et de rapport $\frac{1}{3}$;
3. rotation de centre $\Omega(1)$ et d'angle $\frac{2\pi}{3}$.

7.36. On considère les points A, B, C, P d'affixes respectives $z_A = \frac{3}{2} + 6i$, $z_B = \frac{3}{2} - 6i$, $z_C = -3 - \frac{1}{4}i$ et $z_P = 3 + 2i$, ainsi que le vecteur \vec{w} d'affixe $z_{\vec{w}} = -1 + \frac{5}{2}i$.

1. (a) Calculer l'affixe z_Q de Q , image de B par la translation t de vecteur \vec{w} .
(b) Calculer l'affixe z_R de R , image de P par l'homothétie h de centre C et de rapport $-\frac{1}{3}$.
(c) Déterminer l'affixe z_S du point S , image du point P par la rotation r de centre A et d'angle $-\frac{\pi}{2}$.
2. (a) Démontrer que le quadrilatère $PQRS$ est un parallélogramme.
(b) Calculer $\frac{z_R - z_Q}{z_P - z_Q}$. En déduire la nature précise du parallélogramme $PQRS$.
(c) Montrer que les points P, Q, R, S appartiennent à un même cercle, noté Γ , dont on calculera l'affixe du centre et le rayon.
3. La droite (AP) est-elle tangente à Γ ?

7.37. Soient $A(-1)$ et $B(3i)$. Soit $f : M(z) \neq A \mapsto M'(z')$ où $z' = i \frac{z - 3i}{z + 1}$.

1. Soit $C(2 - i)$. Montrer que C possède un unique antécédent D par f .
2. Déterminer la nature du triangle ABC .
3. Montrer que, pour $M \neq A, B$, on a $OM' = \frac{BM}{AM}$ et $\left(\vec{u}, \overrightarrow{OM'}\right) = \frac{\pi}{2} + \left(\overrightarrow{MA}, \overrightarrow{MB}\right)$.
4. Déterminer l'ensemble \mathcal{E} des points M tels que M' soit sur le cercle trigonométrique.
5. Déterminer l'ensemble \mathcal{F} des points M tels que M' soit sur l'axe réel.

7.38. Soit f la fonction définie sur $[0; 1]$ par $f(x) = x - 2\sqrt{x} + 1$. Montrer, en lui appliquant la rotation de centre O et d'angle $\frac{\pi}{4}$, que la courbe de f est un morceau de parabole.

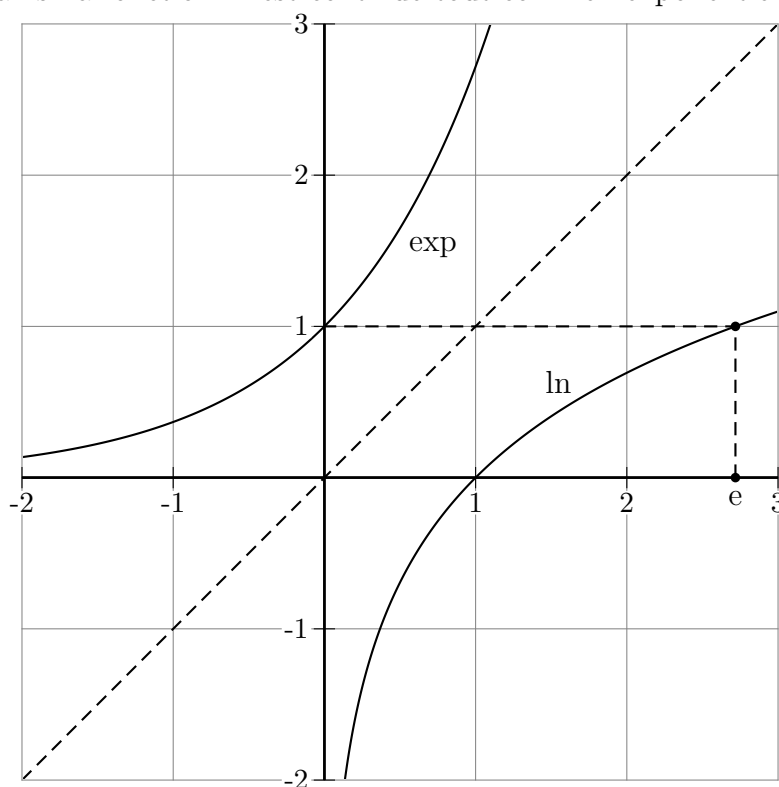
8. Logarithme

8.1 Construction

Définition. L'exponentielle $\exp : \mathbb{R} \rightarrow \mathbb{R}_+^*$ réalise une bijection. La fonction *logarithme népérien* est sa réciproque, notée $\ln : \mathbb{R}_+^* \rightarrow \mathbb{R}$. Ainsi, $y = \ln x \Leftrightarrow x = e^y$.

Remarque. • Le logarithme népérien ne s'applique donc qu'aux réels strictement positifs, ce qui le rend plus délicat à traiter que l'exponentielle, qui est définie, elle, sur \mathbb{R} .

- $\ln 1 = 0$; $\ln e = 1$; $\ln \frac{1}{e} = -1$.
- Quel que soit x , $\ln(e^x) = x$; quel que soit $x > 0$, $e^{\ln x} = x$.
- La courbe de \ln est la symétrique de celle de l'exponentielle par rapport à la première bissectrice, et ainsi la fonction \ln est continue tout comme l'exponentielle :



- L'adjectif *népérien* rend hommage à John Napier (écossais, 1550-1617), inventeur du logarithme.

8.2 Propriétés

8.2.1 Dérivabilité

Théorème. \ln est dérivable sur \mathbb{R}_+^* et quel que soit $x > 0$, $\ln'(x) = \frac{1}{x}$.

Preuve. Soient $x_0 > 0$ et $x > 0$. On pose $y_0 = \ln x_0$ et $y = \ln x$. Le taux de variation de \ln en x_0 vaut $\frac{\ln x - \ln x_0}{x - x_0} = \frac{y - y_0}{\exp y - \exp y_0}$. Lorsque x tend vers x_0 , y tend vers y_0 car le logarithme népérien est continu. Le taux de variation tend donc vers $\frac{1}{\exp' y_0} = \frac{1}{\exp y_0} = \frac{1}{x_0}$. \square

Corollaire. La fonction \ln est strictement croissante sur \mathbb{R}_+^* .

Preuve. $\ln' x = \frac{1}{x} > 0$. (On pouvait aussi utiliser le fait que \ln est la réciproque de \exp qui est strictement croissante.) \square

8.2.2 Relation fonctionnelle caractéristique

Théorème. Soient $x > 0$ et $y > 0$. Alors :

- $\ln(xy) = \ln x + \ln y$, i.e. le logarithme népérien transforme un produit en somme ;
- $\ln \frac{x}{y} = \ln x - \ln y$;
- $\ln \frac{1}{x} = -\ln x$;
- $\ln x^n = n \ln x$ pour $n \in \mathbb{Z}$.

Preuve. L'exponentielle transforme une somme en produit, et le logarithme népérien est sa réciproque. Par acquis de conscience, vérifions : $\ln(xy) = \ln x + \ln y \Leftrightarrow xy = \exp(\ln x) \exp(\ln y) \Leftrightarrow xy = xy$ ce qui est incontestablement vrai.

Les autres propositions se démontrent de la même manière, i.e. en passant à l'exponentielle. \square

Théorème. Soit f une fonction définie et continue sur \mathbb{R}_+^* , vérifiant $f(xy) = f(x) + f(y)$. Alors f est une fonction logarithmique ; si l'on suppose $f(e) = 1$, alors $f = \ln$.

Preuve. Soit $g = f \circ \exp$. Soient x et y deux réels. On vérifie aisément que $g(x+y) = g(x) + g(y)$. On a déjà prouvé par le passé qu'une telle fonction est linéaire, i.e. $g = \alpha \text{Id}$. En composant à droite par \ln , il vient $f = \alpha \ln$. Si maintenant $f(e) = 1$, alors $\alpha = 1$ et donc $f = \ln$. \square

8.2.3 Approximation affine en 1

Théorème.

- L'équation de la tangente en 1 de \ln est $y = x - 1$;
- pour $x \approx 0$, $\ln(1+x) \approx x$.

Preuve.

- La formule $y - \ln 1 = \ln' 1 \cdot (x - 1)$ donne $y = x - 1$ directement.
- L'expression affine de la dérivée donne $\ln(1+x) = \ln 1 + \ln' 1 \cdot x + x\varepsilon(x)$ soit $\ln(1+x) = x + x\varepsilon(x) \approx x$ si x est petit.

\square

8.2.4 Inégalité fondamentale

Théorème. \ln est au-dessous de sa tangente en 1, i.e. quel que soit $x > 0$, $\ln x \leq x - 1$. En particulier, $\ln x < x$.

Preuve. C'est le théorème symétrique du résultat $\exp x \geq 1 + x > x$. \square

8.2.5 Comportement asymptotique

Théorème. • $\lim_{x \rightarrow +\infty} \ln x = +\infty$;

- $\lim_{x \rightarrow 0^+} \ln x = -\infty$;
- $\lim_{x \rightarrow +\infty} \frac{\ln x}{x^n} = 0$;
- $\lim_{x \rightarrow 0^+} x^n \ln x = 0$.

Preuve. Ce ne sont que les propriétés symétriques de celles de l'exponentielle. □

8.2.6 Autres logarithmes

Définition. • Pour $a > 0$, le *logarithme de base a* est défini sur \mathbb{R}_+^* par $\log_a x = \frac{\ln x}{\ln a}$.
• La fonction *logarithme décimal*, notée \log , est le logarithme de base 10.

Remarque. • Ainsi, \log_a a les mêmes propriétés algébriques que \ln , et l'on a $\log_a a = 1$.
• Le logarithme népérien est donc le logarithme en base e puisque $\ln e = 1$.

8.3 Fonctions puissances

8.3.1 Puissance

Définition. Pour $x > 0$ et $y \in \mathbb{R}$, la *puissance* de x par y vaut $x^y = e^{y \ln x}$.

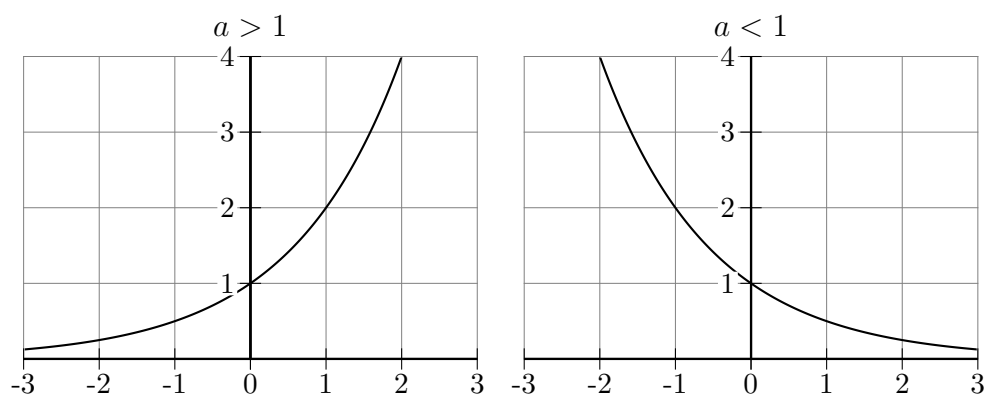
Remarque. • Si $y \in \mathbb{Q}$, cette définition coïncide avec celle d'une puissance rationnelle. En effet, si $y = \frac{p}{q}$ alors la nouvelle définition donne $(x^y)^q = e^{p \ln x}$ et l'ancienne donne $(x^y)^q = x^p$; en prenant le logarithme, on montre que ces deux expressions sont égales.
• Les propriétés usuelles des puissances sont conservées (la preuve est facile).
• La seule différence entre les puissances entières et réelles apparaît pour les nombres négatifs. Par exemple, $(-1)^3$ vaut classiquement -1 mais n'existe pas lors d'un calcul de puissance réelle.
• On peut cependant remarquer très naïvement que $(-1)^3 = (e^{i\pi})^3 = e^{3i\pi} = -1...$
• De manière plus générale, on peut calculer ainsi toute puissance d'un nombre négatif mais en acceptant de sortir du cadre réel.
• On a très simplement $\ln x^y = y \ln x$.

8.3.2 Fonctions exponentielles de base a

Ce sont les fonctions a^x avec $a > 0$ et $x \in \mathbb{R}$.

Étude Pour les étudier, il suffit de noter que, par définition, $a^x = e^{x \ln a}$. Il faut prendre garde à la dérivée, qui est $a^x \ln a$ et non xa^{x-1} . La réciproque de l'exponentielle de base a est bien sûr le logarithme de base a , le plus utilisé étant le logarithme décimal, i.e. de base 10.

Allure



8.3.3 Fonctions puissances

Ce sont les fonctions x^α avec $x > 0$ et $\alpha \in \mathbb{R}$.

Étude Pour les étudier, il suffit de noter que, par définition, $x^\alpha = e^{\alpha \ln x}$. La dérivée est, sans piège cette fois, $\alpha x^{\alpha-1}$.

Allure Les possibilités sont multiples, liées aux signes de la dérivée (sens de variation) et de la dérivée seconde (convexité).

8.4 Exercices

Généralités

8.1. Montrer que $\ln x = \ln y \Leftrightarrow x = y$ et que $\ln x < \ln y \Leftrightarrow x < y$.

8.2. Si $u > 0$ est dérivable, montrer que $(\ln u)' = \frac{u'}{u}$.

8.3. Simplifier les expressions suivantes :

1. $\ln e - 3 \ln 1 + \ln e^4$;
2. $\ln(e\sqrt{e}) + \ln \frac{1}{e}$;
3. $\ln(e + 1) - \ln\left(1 + \frac{1}{e}\right)$;
4. $3 \ln(\sqrt{2} + 1) + \ln(5\sqrt{2} - 7)$.

Résolution d'équations et d'inéquations

8.4. Résoudre dans \mathbb{R} les équations suivantes :

1. $2^{1024} = 10^x$;
2. $\ln(2x - 1) - \ln x = 2$;
3. $\ln(x - 2) + \ln(4 - x) = \ln(2x - 5)$;
4. $\ln(x^2 + 2) = 0$.

8.5. Résoudre dans \mathbb{R} les inéquations suivantes :

1. $2^x > 10^{100}$;
2. $0,3^x < 0,01$;
3. $\ln(2x - 1) > 1$;
4. $\ln(x^2 - 4) > 0$;
5. $\ln(x + 2) \geq 2 \ln x$.

8.6. La croissance du PIB du Royaume Merveilleux des Mathématiques est de 3% par an. Combien d'années vont s'écouler avant le doublement de son PIB ?

8.7. Déterminer les fonctions réciproques de ch et sh sur \mathbb{R}_+ .

8.8. Soit $x > 0$. En supposant qu'il n'y ait pas de problème d'existence, trouver une solution de $x^{x^{x^{\dots}}} = 2$.

Dérivées

8.9. Calculer sans justification les dérivées des fonctions suivantes :

1. $(\ln x)^2$;
2. $\ln(3x^2 + 5)$;
3. $\ln(\cos x)$.

8.10. La fonction f définie sur \mathbb{R}_+ par $f(x) = x^2 \ln x$ et $f(0) = 0$ est-elle dérivable en 0 ?

8.11. Montrer que les courbes de l'exponentielle et du logarithme népérien possèdent deux tangentes communes.

Limites

8.12. Calculer les limites des fonctions suivantes :

1. $\frac{\ln x}{x^2}$ en $+\infty$;
2. $x - \ln x$ en $+\infty$;
3. $\frac{\ln(x+1)}{x+1}$ en $+\infty$;
4. $\frac{\ln x}{x+1}$ en $+\infty$;
5. $\frac{\ln(x^2+1)}{2x+1}$ en $+\infty$;
6. $\frac{\ln x - 1}{x - e}$ en e ;
7. $\frac{\ln(1+5x)}{x}$ en 0 ;
8. $\frac{(\ln x)^2}{x}$ en $+\infty$;

8.13. Calculer la limite en $+\infty$ de $\frac{2^x}{x^2}$.

8.14. Calculer la limite en $+\infty$ de $\left(1 + \frac{1}{n}\right)^n$.

Autres logarithmes

8.15. 1. Étudier les variations de la fonction \log et la représenter rapidement.

2. Calculer $\log 10^x$ pour x réel.

8.16. L'acidité d'une solution est mesurée par $\text{pH} = -\log[H^+]$ où $[H^+]$ est la concentration d'ions H^+ en mol/L.

1. Quelle est la concentration $[H^+]$ d'une solution neutre ($\text{pH} = 7$) ?
2. Comment varie le pH si $[H^+]$ est multipliée par 10 ?

3. Dans 1 litre d'eau neutre, on dilue 1 cl de jus de citron ($\text{pH} = 2,3$). Calculer une bonne approximation du pH de la citronnade.

8.17. 1. Calculer $\log 52$, $\log 666$, $\log 1789$, $\log 150\,000\,000$.

2. Soit N un entier naturel non nul.

Montrer que le nombre de chiffres de l'écriture décimale de N vaut $\lfloor \log N \rfloor + 1$.

3. Combien de chiffres possède le nombre 1492^{1515} en base 10 ?

4. Le plus grand nombre premier connu à ce jour est le nombre de Mersenne $2^{32\,582\,657} - 1$. Combien de chiffres sont nécessaires à son écriture en base 10 ?

5. Le RSA (*dû à Rivest-Shamir-Adleman*) est un algorithme de cryptage dont la sécurité tient en un nombre entier, produit de deux nombres premiers. Si l'on réussit à factoriser ce nombre, le code est brisé. La société *RSA Security* organisait un challenge destiné à factoriser un de leurs nombres. Le plus petit parmi ceux proposés en 2007 était *RSA-704*, i.e. un nombre de 704 bits, récompensé par 30.000 \$.

Combien de chiffres possède-t-il en base 10 ?

Études de fonctions

8.18. Étudier (*limites, variations*) la fonction f définie sur \mathbb{R}_+^* par $f(x) = x^x$.

8.19. Étudier (*limites, variations, ...*) la fonction f définie sur \mathbb{R} par $f(x) = \ln(1 + e^{-x})$.

8.20. Étudier (*limites, variations, ...*) la fonction f définie sur \mathbb{R}_+^* par $f(x) = \frac{1 + \ln x}{x}$.

8.21. On définit la fonction f sur \mathbb{R}_+^* par $f(x) = -3 - \ln x + 2(\ln x)^2$. On note \mathcal{C} sa courbe.

1. (a) Résoudre l'équation $f(x) = 0$.

(b) Résoudre l'inéquation $f(x) > 0$.

2. (a) Déterminer les limites de f en 0 et en $+\infty$.

(b) Étudier le sens de variation de f et dresser son tableau.

3. Déterminer une équation de la tangente \mathcal{T} à \mathcal{C} au point d'abscisse $e^{\frac{5}{4}}$.

4. On veut étudier la position relative de \mathcal{C} par rapport à \mathcal{T} .

On pose $\Delta(x) = f(x) - \left(4e^{-\frac{5}{4}}x - \frac{41}{8}\right)$.

(a) Montrer que $\Delta'(x) = \frac{4 \ln x - 1}{x} - 4e^{-\frac{5}{4}}$ puis calculer $\Delta''(x)$.

(b) Étudier le sens de variation de Δ' et en déduire que $\Delta'(x) \leq 0$.

(c) Déterminer le signe de $\Delta(x)$ et en déduire la position de \mathcal{C} par rapport à \mathcal{T} .

9. Conditionnement et indépendance

9.1 Espaces probabilisés

9.1.1 Évènements

Définition. • L'univers Ω d'une expérience aléatoire est l'ensemble constitué des résultats possibles de cette expérience ;

- un évènement est une partie de Ω ;
- l'ensemble $\mathcal{P}(\Omega)$ des parties de Ω est constitué de tous les évènements ;
- une issue est un élément de Ω ;
- un évènement élémentaire est un évènement composé d'une seule issue.

Définition. Soient A et B deux évènements.

- $A \cup B$ est la réunion de A et B , constituée des éléments de Ω qui sont dans A ou B ;
- $A \cap B$ est l'intersection de A et B , constituée des éléments de Ω qui sont dans A et B ;
- \bar{A} est le contraire de A , i.e. son complémentaire dans Ω ;
- A et B sont incompatibles lorsque $A \cap B = \emptyset$, i.e. lorsqu'ils sont disjoints.

Définition. L'ensemble d'évènements $\{A_k\}_k$ est une partition de l'évènement B lorsque :

- les A_k sont deux à deux incompatibles ;
- la réunion des A_k est égale à B .

9.1.2 Probabilités

Définition. Une probabilité sur un univers Ω fini est une application $P : \mathcal{P}(\Omega) \rightarrow [0; 1]$, qui associe à un évènement A un nombre $P(A)$, vérifiant :

- $P(\Omega) = 1$ (normalisation) ;
- si $A = \{\omega_1, \dots, \omega_n\}$ alors $P(A) = \sum_{k=1}^n P(\{\omega_k\})$ (σ -additivité, i.e. la probabilité d'un évènement est la somme des probabilités des évènements élémentaires qui le composent).

Théorème. • $0 \leq P(A) \leq 1$;

- $P(A \cup B) = P(A) + P(B) - P(A \cap B)$;
- $P(\bar{A}) = 1 - P(A)$;
- si $\{A_k\}_k$ est une partition de B alors $P(B) = \sum_k P(A_k)$;
- en particulier, si $\{A_k\}_k$ est une partition de Ω alors $\sum_k P(A_k) = 1$.

9.1.3 Variables aléatoires

Définition. Une variable aléatoire (v.a.) sur un univers Ω est une application $X : \Omega \rightarrow \mathbb{R}$, qui associe à une issue ω un nombre réel $X(\omega)$.

- Remarque.**
- Aucune contrainte n'est imposée à une v.a., du moins au niveau lycée ;
 - une v.a. sert à exploiter numériquement le résultat brut d'une expérience aléatoire ;
 - si Ω est fini alors une v.a. sur Ω prend un nombre fini de valeurs.

Définition. Soient a un réel et A un ensemble de réels. On pose :

- $\{X = a\} = \{\omega \in \Omega, X(\omega) = a\}$;
- $\{X \in A\} = \{\omega \in \Omega, X(\omega) \in A\}$.

9.2 Conditionnement et indépendance

On se place dans un espace probabilisé (Ω, P) .

9.2.1 Conditionnement

Considérons deux évènements A et B . Réalisons un certain nombre de fois une même expérience aléatoire et notons $f_{A \cap B}$, f_A et f_B les fréquences de réalisations de $A \cap B$, A et B . Par exemple, considérons le résultat d'expériences suivant :

n	1	2	3	4	5	6
A	×			×	×	×
B		×		×		×

La fréquence de $A \cap B$ vaut $\frac{2}{6}$, celle de A vaut $\frac{4}{6}$, celle de B vaut $\frac{3}{6}$.

La fréquence relative de A par rapport à B vaut $\frac{f_{A \cap B}}{f_B}$, ce qui donne $\frac{2/6}{3/6} = \frac{2}{3}$. On peut noter qu'il est plus judicieux d'observer directement que la fréquence de A sachant que B est réalisé est de $\frac{2}{3}$ (lors des 3 réalisations de B , A a été réalisé 2 fois).

Définition. Soient A et B deux évènements avec $P(B) \neq 0$.

- La probabilité de A sachant B est $P_B(A) = P(A|B) = \frac{P(A \cap B)}{P(B)}$;
- P_B est la *probabilité conditionnelle* sachant B .

Remarque. P_B est bien une probabilité (il est facile de vérifier les deux items de la définition d'une probabilité) induite par B sur Ω , et non pas une probabilité sur B .

9.2.2 Indépendance

Remarque. Si A et B sont deux évènements de probabilités non nulles, on peut penser qu'ils sont indépendants (au sens usuel du terme) si les probabilités de leurs réalisations ne dépendent pas l'une de l'autre : $P_B(A) = P(A)$ par exemple. Ceci donne $\frac{P(A \cap B)}{P(B)} = P(A)$ soit $P(A \cap B) = P(A)P(B)$.

Définition. Deux évènements A et B sont *indépendants* si $P(A \cap B) = P(A)P(B)$.

Théorème. Lors d'une répétition d'expériences aléatoires indépendantes, la probabilité de la liste des résultats est le produit des probabilités individuelles de ces résultats.

Définition. On se place dans un univers fini. Deux v.a. X et Y sont *indépendantes* si les évènements $\{X = x_i\}$ et $\{Y = y_j\}$ sont indépendants pour toutes valeurs x_i de X et y_j de Y .

Corollaire. Si les deux v.a. X et Y sont indépendantes alors $P(\{X = x_i\} \cap \{Y = y_j\}) = P(\{X = x_i\})P(\{Y = y_j\})$ pour toutes valeurs x_i de X et y_j de Y .

9.2.3 Corrélation et causalité

- La notion d'indépendance dépend de la probabilité choisie. Par exemple lançons un dé tétraédrique équilibré et considérons les évènements $A = \{1, 2\}$ et $B = \{2, 3\}$. Il est facile de voir que A et B sont indépendants. Si maintenant on pipe notre dé en changeant les probabilités de 1,2,3,4 en $\frac{1}{4}, \frac{1}{4}, \frac{1}{3}, \frac{1}{6}$, alors dans ce cas les deux évènements A et B ne sont plus indépendants.
- Le théorème sur la probabilité d'une liste de résultats, bien que simple à retenir, est quelque peu énoncé de manière biaisée. En effet, la probabilité-produit est justement construite de sorte à ce que la probabilité d'une liste soit le produit des probabilités élémentaires! Par exemple lançons indépendamment deux fois un dé. Il est facile de voir que les évènements $\{(1, y)\}$ et $\{(x, 1)\}$ sont indépendants. Mais la question à se poser est : comment est donc définie la probabilité sur cette expérience aléatoire? Ici, on définit $P(x, y) = \frac{1}{6} \times \frac{1}{6} = \frac{1}{36}$ afin de respecter l'indépendance des deux lancers. Donc nécessairement le théorème précédent sera vérifié...
- On a vu que l'indépendance est liée à la probabilité. La probabilité « naturelle » respecte la notion intuitive d'indépendance puisqu'elle a justement été construite afin de la respecter!
- Attention à ne pas confondre corrélation (i.e. dépendance au sens probabiliste) et causalité (au sens physique)!
 - La chaleur estivale est indéniablement corrélée à la survenue du Tour de France cycliste. Pourtant il n'existe pas de lien de causalité entre ces deux évènements.
Corrélation n'implique pas causalité!
 - La météo est un système chaotique, sensible à de petites variations des conditions initiales. La position de Vénus dans le ciel à un instant donné et le temps qu'il fait un mois plus tard sont liés par une relation de causalité. Les facteurs jouant sur la météo sont pourtant trop nombreux pour qu'une quelconque corrélation existe entre ces deux évènements.
Causalité n'implique pas corrélation!

9.3 Probabilités totales

On se place dans un espace probabilisé (Ω, P) .

9.3.1 Formule des probabilités totales

Lorsqu'un évènement est complexe, sa probabilité peut être difficile à calculer et l'on peut être amené à décomposer l'évènement et le calcul de sa probabilité.

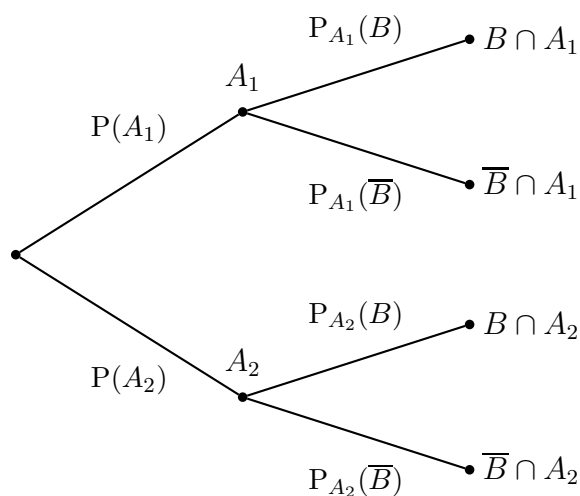
Théorème (formule des probabilités totales). Si $\{A_1, \dots, A_n\}$ est une partition de Ω avec $P(A_k) \neq 0$ pour tout k alors la probabilité d'un évènement B est donnée par

$$P(B) = P_{A_1}(B)P(A_1) + \dots + P_{A_n}(B)P(A_n).$$

Preuve. $\{B \cap A_1, \dots, B \cap A_n\}$ est une partition de B puisque ses évènements sont incompatibles (car les A_k le sont) et leur union donne $(B \cap A_1) \cup \dots \cup (B \cap A_n) = B \cap (A_1 \cup \dots \cup A_n) = B \cap \Omega = B$. Par conséquent $P(B) = P(B \cap A_1) + \dots + P(B \cap A_n) = P_{A_1}(B)P(A_1) + \dots + P_{A_n}(B)P(A_n)$. \square

9.3.2 Arbres

La formule des probabilités totales montre rigoureusement les propriétés classiques de calcul sur les arbres de probabilité.



Ici $P(B)$ est la somme des chemins aboutissant à B , les branches successives d'un chemin étant multipliées. Au passage, faire un arbre permet de se souvenir de la formule...

9.4 Exercices

Sauf mention contraire, on se place dans un espace probabilisé (Ω, P) .

Généralités

- 9.1.** 1. Soient A , B et C trois évènements. Montrer que $P(A \cup B \cup C) = P(A) + P(B) + P(C) - P(A \cap B) - P(A \cap C) - P(B \cap C) + P(A \cap B \cap C)$ en faisant un diagramme.
2. Conjecturer la *formule de Poincaré* donnant $P(A_1 \cup \dots \cup A_n)$ puis la prouver par récurrence.
- 9.2.** Soient A et B deux évènements.
1. Montrer rigoureusement que $\overline{A} \cap B = B - A \cap B$ en s'aidant d'un diagramme.
2. Si A et B sont incompatibles, \overline{A} et B le sont-ils également ?
3. Si A et B sont indépendants, \overline{A} et B le sont-ils également ?
- 9.3.** Soient A et B deux évènements.
1. Montrer rigoureusement que $\overline{A} \cap \overline{B} = \overline{A \cup B}$ en s'aidant d'un diagramme.
2. Si A et B sont incompatibles, \overline{A} et \overline{B} le sont-ils également ?
3. Si A et B sont indépendants, \overline{A} et \overline{B} le sont-ils également ?
- 9.4.** On jette trois pièces. Déterminer l'évènement contraire de :
1. « obtenir au moins une fois pile » ;
2. « obtenir pile à chaque fois » ;
3. « obtenir exactement une fois pile ».
- 9.5.** Soient A et B deux évènements avec $P(A) = 0,2$, $P(B) = 0,5$ et $P(A \cup B) = 0,6$.
1. A et B sont-ils incompatibles ?
2. Calculer $P(\overline{A})$, $P(\overline{B})$ et $P(A \cap \overline{B})$.
- 9.6.** Soient A et B deux évènements avec $P(A) = 0,1$, $P(B) = 0,6$ et $P(A \cup B) = 0,65$.
1. Calculer $P(A \cap B)$, $P_B(A)$ et $P_A(B)$.
2. Les évènements A et B sont-ils indépendants ?
- 9.7.** Calculer la probabilité qu'au moins deux élèves aient le même jour d'anniversaire dans une classe de 30.
- 9.8.** Dans un atelier, deux machines produisent les mêmes pièces, au nombre total de 1000. La première en fournit les $4/5$. De plus, 5% des pièces produites par la première machine sont défectueuses et 4% pour la seconde.
1. Construire le tableau de Karnaugh des effectifs.
2. On tire une pièce au hasard. Soient A =« la pièce est produite par la première machine », B =« la pièce est produite par la seconde » et C =« la pièce est défectueuse ». Calculer $P(A)$, $P(B)$, $P(C)$, $P(A \cap C)$ et $P(A \cup C)$.

Conditionnement et indépendance

9.9. On lance un dé. Calculer la probabilité que la face soit supérieure à 4 sachant qu'elle est supérieure à 3.

9.10. On tire une carte d'un jeu de 32.

1. Calculer la probabilité que ce soit un pique sachant que c'est un roi.
2. Calculer la probabilité que ce soit un roi sachant que c'est un pique.
3. Les événements « tirer un roi » et « tirer un pique » sont-ils indépendants ?

9.11. Le lycée général d'Ugine compte 410 élèves dont 15% de filles. Seuls 30% des garçons et 40% des filles savent où se trouve le mont Charvin. On interroge un élève pris au hasard.

1. Calculer la probabilité que cet élève soit une fille qui sait où se trouve le mont Charvin.
2. Calculer la probabilité que cet élève soit une fille qui ne sait pas où se trouve le mont Charvin.
3. Sachant que l'élève interrogé sait où se trouve le mont Charvin, calculer la probabilité que ce soit une fille.

9.12. On lance une pièce quatre fois de suite.

1. Calculer la probabilité d'obtenir pile quatre fois.
2. Calculer la probabilité d'obtenir au moins une fois pile.
3. Calculer la probabilité d'obtenir exactement une fois pile.
4. Calculer la probabilité d'obtenir pile et face en alternance.

9.13. Le chevalier de Méré posa la question suivante à Pascal : « Est-il plus probable d'obtenir au moins une fois 6 quand on lance un dé quatre fois de suite, ou d'obtenir au moins un double 6 quand on lance deux dés vingt-quatre fois de suite » ?

Qu'en est-il ? Pourquoi le chevalier n'arrivait-il pas à répondre par l'expérience à son problème ?

9.14. Un dixième de la population française a été vacciné contre la grippe saisonnière. On constate qu'il y a 25% de vaccinés parmi les malades. On sait aussi qu'il y a 8% de malades parmi les vaccinés. Calculer la probabilité d'attraper la grippe pour un individu non vacciné.

- 9.15.**
1. Trois chasseurs tirent de façon indépendante sur trois canards. Ils sont sûrs d'atteindre leur cible. Calculer les probabilités que les trois canards soient touchés puis qu'un seul canard soit touché.
 2. Dix canards, dont un nommé Mario, vaquent à leurs banales occupations de canards. Dix chasseurs tirent, de façon indépendante, sur ce groupe de canards. Chacun d'eux est sûr d'atteindre sa cible. Calculer la probabilité que Mario soit touché.

9.16. On dispose d'une urne contenant une boule rouge et deux boules bleues. On tire successivement et sans remise les trois boules.

1. Construire l'arbre de cette expérience.

2. Soit X le rang de tirage de la boule rouge. Déterminer la loi de X .
3. Soit Y la couleur de la dernière boule tirée, en comptant 1 pour rouge et 2 pour bleue. Déterminer la loi de Y .
4. Les v.a. X et Y sont-elles indépendantes ?

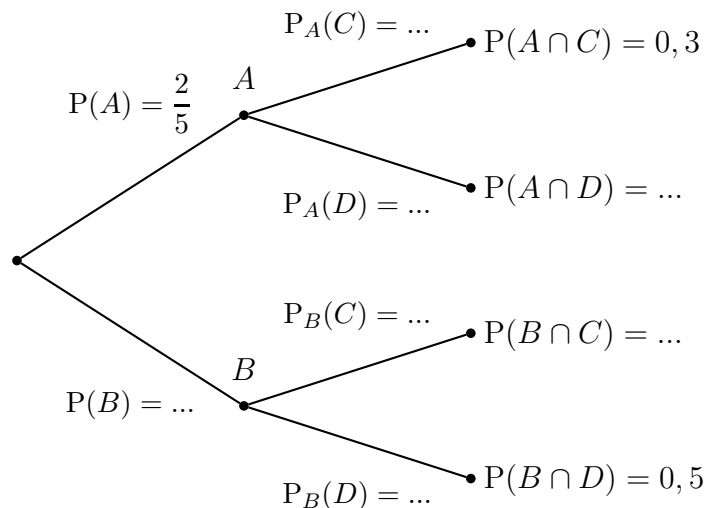
9.17. On jette simultanément trois dés.

La modélisation est plus aisée si on les suppose discernables.

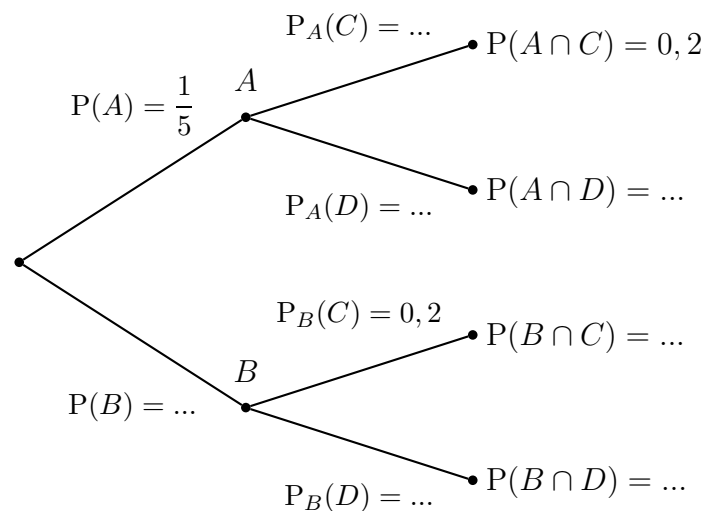
1. Modéliser l'expérience, i.e. donner Ω et P .
2. Calculer la probabilité d'obtenir au moins un « 1 ».
3. Calculer la probabilité d'obtenir au moins deux faces portant le même chiffre.
4. Calculer la probabilité que la somme des trois faces soit paire.
5. Les événements considérés aux deux questions précédentes sont-ils indépendants ?

Probabilités totales

9.18. Compléter l'arbre :



9.19. Compléter l'arbre :



9.20. On dispose de 1000 pièces de monnaie : 999 normales et 1 possédant 2 côtés « pile ». On tire au hasard une pièce, et on la lance 10 fois de suite.

1. Calculer la probabilité d'obtenir 10 fois « pile ».
2. Sachant qu'on a obtenu 10 fois « pile », quelle est la probabilité qu'on ait tiré la fausse pièce ?

9.21. Un candidat doit répondre à une question pour laquelle on lui donne trois réponses possibles dont une seule est bonne. Le candidat connaît les trois quarts des réponses, mais peut aussi répondre au hasard.

1. Quelle est la probabilité que le candidat connaisse la bonne réponse sachant qu'il a bien répondu ?
2. Donner une relation entre les ratios de réponses connues du candidat et de bonnes réponses.

9.22. On se donne un carré $ABCD$ de centre O . Un ragondin, nommé Alfred, se déplace aléatoirement d'un point à un autre du carré en suivant les segments formés par $OABCD$. Alfred part du point A . Le point O est muni d'un klaxon qu'Alfred aime faire fonctionner. On note p_n la probabilité qu'Alfred klaxonne pour la première fois au n -ième déplacement.

1. Calculer p_1 .
2. Justifier que $p_n = \left(\frac{2}{3}\right)^{n-1} \times \frac{1}{3}$.
3. Soit K_n l'évènement « Alfred klaxonne au moins une fois au bout de ses n premiers déplacements ».
 - (a) On note $S_n = p_1 + \dots + p_n$. Montrer que $P(K_n) = S_n$.
 - (b) Calculer S_n . Pouvait-on prévoir plus facilement ce résultat ?
 - (c) Calculer la limite de S_n et interpréter le résultat.

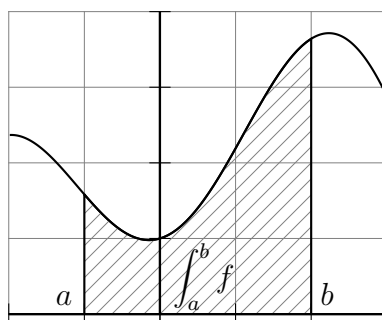
10. Intégration

10.1 Intégrale d'une fonction continue

10.1.1 Intégrale d'une fonction positive

Définition. Soit f une fonction continue et positive sur un intervalle $[a; b]$.

- Le *domaine sous \mathcal{C}_f* entre a et b est le domaine délimité par les droites d'équations $x = a$ et $x = b$, l'axe des abscisses et la courbe \mathcal{C}_f ;
- l'*aire sous f* entre a et b est l'aire de ce domaine ;
- l'*intégrale* de f entre a et b est cette aire, notée $\int_a^b f$ ou $\int_a^b f(x) \, dx$.



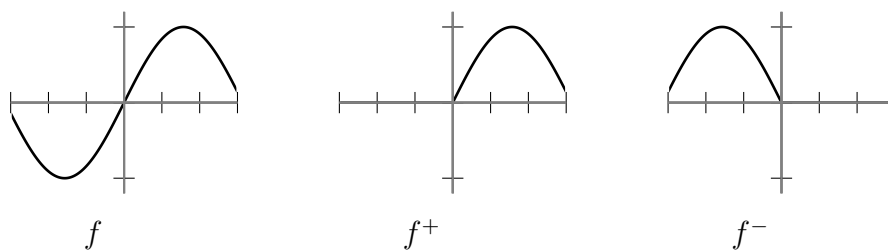
Remarque. Il faudrait définir correctement la notion intuitive d'aire. Ce n'est pas au programme et conduirait à la construction de l'intégrale de Riemann, dont nous verrons l'idée lors de l'étude de la méthode des rectangles.

- Remarque.**
- Le symbole \int est une déformation de l'ancien « S », et $\int_a^b f$ se lit souvent « somme de f entre a et b » ;
 - a et b sont les *bornes* de l'intégrale ;
 - dans $\int_a^b f(x) \, dx$, x est une variable muette : elle ne joue qu'un rôle pratique et on pourra très bien noter $\int_a^b f(\xi) \, d\xi$ si l'envie nous en prend ;
 - on peut cependant interpréter $\int_a^b f(x) \, dx$ comme la somme des aires $f(x)dx$ des rectangles infinitésimaux de largeur dx et de hauteur $f(x)$;
 - $\int_a^a f = 0$ puisque l'aire d'un segment est nulle.

10.1.2 Intégrale d'une fonction de signe quelconque

Définition. Soit f une fonction continue.

- La partie positive de f est définie par $f^+(x) = f(x)$ si $f(x) > 0$ et $f^+(x) = 0$ sinon ;
- La partie négative de f est définie par $f^-(x) = -f(x)$ si $f(x) < 0$ et $f^-(x) = 0$ sinon.

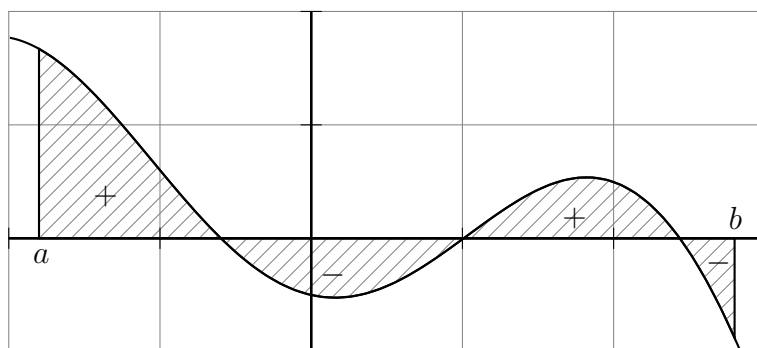


Remarque.

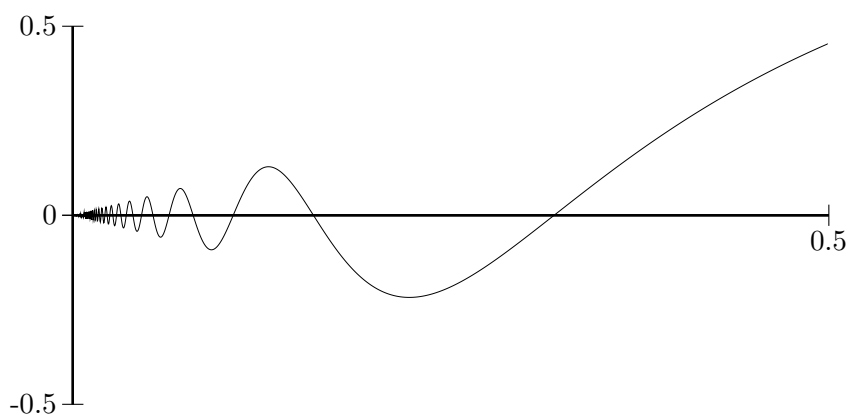
- Ainsi on a $f = f^+ - f^-$;
- $f = f^+$ et f^- sont des fonctions continues positives.

Définition. Soit f une fonction continue sur $[a; b]$. L'intégrale de f entre a et b est le nombre

$$\int_a^b f = \int_a^b f^+ - \int_a^b f^-$$



Remarque. Il existe malheureusement des fonctions continues exotiques, telles que $f(x) = x \sin \frac{1}{x}$ si $x \neq 0$ et $f(0) = 0$:



Ici f change de signe une infinité de fois sur l'intervalle pourtant fini $[0; 0, 5]$ et transforme notre *somme* d'aires positives et négatives en une *série*, i.e. une somme infinie. Ce type de fonction sera donc banni pour le moment...

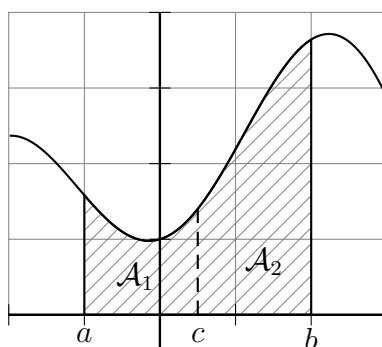
10.2 Propriétés

10.2.1 Opérations

Définition. Soit f une fonction continue sur un intervalle $[a; b]$. On pose, en cohérence avec la relation de Chasles ci-dessous, $\int_b^a f = -\int_a^b f$.

Théorème (relation de Chasles). Soit f une fonction continue sur un intervalle contenant a , b et c . Alors $\int_a^c f + \int_c^b f = \int_a^b f$.

Preuve. Notons qu'il suffit de montrer ce résultat pour une fonction positive. Considérons le cas le plus clair ; ici on a bien $\int_a^b f = \mathcal{A}_1 + \mathcal{A}_2 = \int_a^c f + \int_c^b f$:



□

Théorème (linéarité). Soient f et g deux fonctions continues sur des intervalles contenant a et b . Alors :

- $\int_a^b f + g = \int_a^b f + \int_a^b g$;
- $\int_a^b \lambda f = \lambda \int_a^b f$ pour tout réel λ .

Preuve. Il suffit de raisonner en termes d'aires (cf relation de Chasles), en laissant la rigueur de côté. □

Remarque. Malheureusement, il est important de noter que :

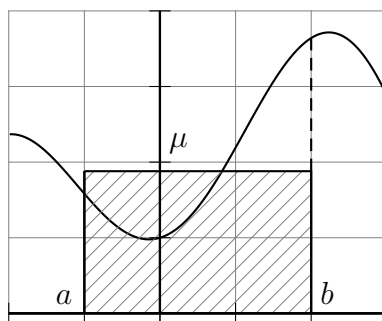
$$\int_a^b fg \neq \left(\int_a^b f \right) \left(\int_a^b g \right)$$

L'intégration par parties, que nous verrons ultérieurement, permettra parfois de calculer l'intégrale d'un produit.

10.2.2 Valeur moyenne et interprétations physiques

Définition. Soit f une fonction continue et positive sur un intervalle $[a; b]$. La *valeur moyenne* de f sur $[a; b]$ est le nombre $\mu = \frac{1}{b-a} \int_a^b f$.

Remarque. Ainsi, l'aire du rectangle $[0; \mu] \times [a; b]$ est égale à l'aire sous f entre a et b .



En effet, on a par définition $\mu(b-a) = \int_a^b f$. De même, l'aire supérieure entre f et μ est égale à l'aire inférieure, en remarquant que $\int_a^b (f - \mu) = \int_a^b f - \int_a^b \mu = \int_a^b f - \mu(b-a) = 0$.

Remarque. • Considérons un mobile sur une droite, de vitesse instantanée $v(t) > 0$. Alors la distance parcourue par ce mobile entre les temps t_0 et t_1 vaut

$$d = v_{\text{moy}}(t_1 - t_0) = (t_1 - t_0) \frac{1}{t_1 - t_0} \int_{t_0}^{t_1} v(t) dt = \int_{t_0}^{t_1} v(t) dt.$$

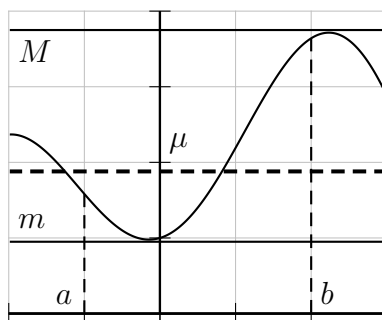
L'unité de la grandeur d est celle de $v(t)$ multipliée par celle de t , soit $m.s^{-1}.s = m$. L'unité de la vitesse moyenne est bien celle de $v(t)$ puisque $s^{-1}.m = m.s^{-1}$.

- La quantité de courant d'intensité $i(t) > 0$ passant par un fil entre les temps t_0 et t_1 vaut $\int_{t_0}^{t_1} i(t) dt$. Ainsi, la différence de potentiel d'un condensateur $u = \frac{1}{C} \int_{t_0}^{t_1} i(t) dt$ est tout simplement proportionnelle à la quantité d'électrons stockée.

10.2.3 Inégalités

Théorème. Soient f et g deux fonctions continues sur $[a; b]$.

- (positivité) Si $f \geq 0$ alors $\int_a^b f \geq 0$;
- (préservation de l'ordre) si $f \leq g$ alors $\int_a^b f \leq \int_a^b g$;
- (inégalités de la moyenne)
 - si $m \leq f \leq M$ alors $m(b-a) \leq \int_a^b f \leq M(b-a)$;
 - si $m \leq f \leq M$ alors $m \leq \mu \leq M$;
 - si $|f| \leq M$ alors $\left| \int_a^b f \right| \leq M(b-a)$.



Preuve. • Si f est positive alors l'aire sous f est par définition positive.

- $g - f \geq 0$ donc $\int_a^b (g - f) \geq 0$, ou encore $\int_a^b g - \int_a^b f \geq 0$.
- $m \leq f \leq M$ donc $\int_a^b m \leq \int_a^b f \leq \int_a^b M$, soit $m(b - a) \leq \int_a^b f \leq M(b - a)$.
 - En divisant par $b - a$ il vient $m \leq \mu \leq M$.
 - $|f| \leq M \Leftrightarrow -M \leq f \leq M$ et donc $-M(b - a) \leq \int_a^b f \leq M(b - a)$. Il suffit ensuite de passer à la valeur absolue.

□

10.3 Calcul d'intégrales

Nous ne savons calculer pour l'instant que des intégrales de fonctions dont les courbes ont des formes géométriques simples.

10.3.1 Primitives

Définition. Soit f une fonction définie sur un intervalle I . Une *primitive* de f sur I est une fonction F dérivable sur I telle que $F' = f$.

Théorème. Une fonction f admettant une primitive F sur un intervalle I possède une infinité de primitives sur I , toutes de la forme $F + k$ où k est une constante réelle.

Preuve. Si $G = F + k$ alors $G' = F' = f$. Réciproquement, si G est une primitive de f alors $(G - F)' = G' - F' = f - f = 0$ sur I . Ainsi $G - F$ est une constante k , i.e. $G = F + k$. □

Remarque. Toutes les courbes des primitives de f se déduisent ainsi les unes des autres par une translation verticale.

Théorème. Si f possède des primitives sur I alors il en existe une seule F vérifiant $F(x_0) = y_0$.

Preuve. C'est une simple conséquence de la remarque précédente. □

10.3.2 Lien entre intégrale et primitive

Théorème. Soit f une fonction continue sur un intervalle I et soit $a \in I$. La fonction $F : I \rightarrow \mathbb{R}$ définie par $F(x) = \int_a^x f$ est l'unique primitive de f sur I qui s'annule en a .

Remarque. Mettons pour le moment la rigueur de côté. On peut constater que $F(x + dx) - F(x) = \int_a^{x+dx} f - \int_a^x f = \int_x^{x+dx} f$. C'est donc l'aire signée d'un rectangle infinitésimal situé à l'abscisse x , de largeur dx et de hauteur $f(x)$. Ainsi $F(x + dx) - F(x) = f(x)dx$; autrement dit, $dF = f(x)dx$, ou encore $\frac{dF}{dx} = f(x)$. La dérivée de F est donc f .

Preuve. On se contente du cas où f est croissante. Notons déjà que F est bien définie sur I car f est continue. Montrons ensuite que F est dérivable en un point $x_0 \in I$.

- Supposons $x > x_0$. Pour $t \in [x_0; x]$ on a $f(x_0) \leq f(t) \leq f(x)$ car f est croissante. En intégrant entre x_0 et x par rapport à t , il vient $f(x_0)(x - x_0) \leq \int_{x_0}^x f(t) dt \leq f(x)(x - x_0)$ en utilisant une inégalité de la moyenne. Ainsi, $F(x) - F(x_0) = \int_a^x f(t) dt - \int_a^{x_0} f(t) dt = \int_{x_0}^x f(t) dt$. On tire donc $f(x_0) \leq \frac{F(x) - F(x_0)}{x - x_0} \leq f(x)$ puisque $x - x_0 > 0$. En faisant tendre x vers x_0 , $f(x)$ tend vers $f(x_0)$ car f est continue, et le théorème d'encadrement montre alors que $\lim_{x \rightarrow x_0^+} \frac{F(x) - F(x_0)}{x - x_0} = f(x_0)$, i.e. F est dérivable à droite en x_0 et $F'(x_0^+) = f(x_0)$.
- Si $x < x_0$, on procède de même et l'on obtient $F'(x_0^-) = f(x_0)$.
- Pour finir, F s'annule bien en a puisque $F(a) = \int_a^a f = 0$.

□

Corollaire (fondamental). Une fonction continue sur un intervalle I possède une infinité de primitives sur I .

Théorème (fondamental du calcul intégral). Si f est une fonction continue sur un intervalle I contenant a et b alors

$$\int_a^b f = F(b) - F(a) = [F(t)]_a^b$$

où F est une primitive quelconque de f sur I .

Preuve. Soit $F(x) = \int_a^x f$. La fonction F est bien une primitive de f sur I et l'on a $F(b) - F(a) = \int_a^b f - 0 = \int_a^b f$. Si $G = F + k$ est une autre primitive de f sur I alors $G(b) - G(a) = (F(b) + k) - (F(a) + k) = F(b) - F(a)$, et ainsi le choix de la primitive n'importe pas. □

10.3.3 Intégration par parties

Nous avons vu que l'intégrale d'un produit ne vaut en général pas le produit des intégrales. La méthode d'intégration suivante fournit une possibilité du calcul de l'intégrale d'un produit.

Théorème (intégration par parties). Soient f et g deux fonctions dérivables sur un intervalle contenant a et b et dont les dérivées sont elles-mêmes continues (i.e. f et g sont de classe C^1). Alors :

$$\int_a^b fg' = [fg]_a^b - \int_a^b f'g$$

Preuve. Souvenons-nous que $(fg)' = f'g + fg'$. Il suffit ensuite d'intégrer cette égalité entre a et b après avoir constaté que les fonctions considérées sont continues. □

Remarque. • Le but de cette formule est d'obtenir l'intégrale du membre de droite plus simple que l'intégrale initiale.

- On peut résumer la formule en $\int uv' = [uv] - \int u'v$. Si l'on met des bornes, on considère des intégrales ; sinon, on considère des primitives.

10.4 Exercices

Généralités

10.1. Soit f la fonction définie sur \mathbb{R} par $f(x) = k > 0$. Calculer $\int_a^b f$.

10.2. Soit f la fonction définie sur \mathbb{R} par $f(x) = |x|$. Calculer $\int_{-1}^2 f$.

10.3. Soit f la fonction définie sur $[-1; 1]$ par $f(x) = \sqrt{1 - x^2}$. Calculer $\int_{-1}^1 f$.

10.4. 1. Évaluer sans calcul $\int_{-\pi}^{\pi} \sin x \, dx$.

2. Quelle est la valeur moyenne d'une fonction continue impaire sur un intervalle symétrique par rapport à 0 ?

10.5. Calculer la valeur moyenne du signal triangulaire $f(x) = 1 - |x - 1|$ entre 0 et 2.

10.6. Montrer que $\left| \int_a^b f \right| \leq \int_a^b |f|$.

10.7. Déterminer toutes les fonctions $f : [0; 1] \rightarrow [0; 1]$ continues vérifiant $\int_0^1 f = \int_0^1 f^2$.

10.8. Étudier la limite de la suite de terme général $u_n = \int_n^{n+1} e^{-x} \, dx$.

Primitives

10.9. 1. Montrer que les fonctions définies par $\frac{x}{3x+1}$ et $-\frac{1}{3} \frac{1}{3x+1}$ sont des primitives sur un même intervalle de la fonction définie par $\frac{1}{(3x+1)^2}$.

2. Diffèrent-elles simplement d'une constante ?

10.10. Montrer que la *fonction de Heaviside*, i.e. valant 0 sur \mathbb{R}_-^* et 1 sur \mathbb{R}_+ , ne possède pas de primitive sur \mathbb{R} .

10.11. Dresser le tableau des primitives de référence de $\frac{1}{2\sqrt{x}}$, x^α (avec $\alpha \neq -1$), $\frac{1}{x}$, e^x , $\sin x$, $\cos x$, $1 + \tan^2 x = \frac{1}{\cos^2 x}$.

10.12. Calculer les primitives des fonctions suivantes, en précisant l'intervalle considéré :

1. $f(x) = x$;

2. $f(x) = x^3$;

3. $f(x) = 3x^5 + 1$;

4. $f(x) = \sqrt{x}$;

5. $f(x) = 7 \cos x - 2 \sin x$;

6. $f(x) = \frac{1}{x^2}$;

7. $f(x) = \frac{1}{\sqrt{x}}$.

10.13. Dresser le tableau des primitives de référence de $u'e^u$, $\frac{u'}{2\sqrt{u}}$, $-\frac{u'}{u^2}$, $u'u^\alpha$ (avec $\alpha \neq -1$), $\frac{u'}{u}$, $u' \cos u$, $u' \sin u$.

10.14. Calculer les primitives des fonctions suivantes, en précisant l'intervalle considéré :

1. $f(x) = \frac{2x}{x^2 + 1}$;

2. $f(x) = \frac{x}{\sqrt{x^2 + 1}}$;

3. $f(x) = \frac{x}{\sqrt{3x^2 + 1}}$;

4. $f(x) = \frac{x^3}{(x^4 + 1)^2}$;

5. $f(x) = \sin x \cos^3 x$;

6. $f(x) = \tan x = \frac{\sin x}{\cos x}$;

7. $f(x) = x\sqrt{x}$;

8. $f(x) = \frac{\sin x}{\cos^2 x}$;

9. $f(x) = (x + 1)e^{x^2 + 2x + 1}$.

10.15. Calculer les primitives des fonctions suivantes, en précisant l'intervalle considéré :

1. $f(x) = \frac{x}{x - 1}$;

2. $f(x) = \sin^2 x$;

3. $f(x) = \cos^4 x$;

4. $f(x) = \frac{1}{1 + e^{-x}}$;

5. $f(x) = \cos 5x \sin 3x$.

10.16. Calculer les intégrales suivantes :

1. $\int_0^1 e^x \, dx$;

2. $\int_0^1 \frac{e^x}{1 + e^x} \, dx$;

3. $\int_0^1 \frac{1}{x - 2} \, dx$;

4. $\int_0^1 \frac{2x + 1}{x^2 + x + 3} \, dx$;

5. $\int_0^{\frac{\pi}{2}} \sin x \cos x \, dx$;

6. $\int_1^e \frac{\ln x}{x} \, dx$.

10.17. Soit f la fonction définie sur $\mathbb{R} - \{1\}$ par $f(x) = \frac{2x-3}{(x-1)^3}$.

1. Déterminer les deux réels a et b vérifiant $f(x) = \frac{a}{(x-1)^2} + \frac{b}{(x-1)^3}$.
2. En déduire une primitive de f sur $]1; +\infty[$.

10.18. Calculer $\int_{-2}^2 \frac{x^2 + 2x - 1}{x + 3} \, dx$.

10.19. Calculer $I = \int_0^{\frac{\pi}{2}} \cos^2 x \, dx$ et $J = \int_0^{\frac{\pi}{2}} \sin^2 x \, dx$ en considérant $I + J$ et $I - J$.

10.20. Soit f une fonction continue sur \mathbb{R} .

1. Si f est impaire, montrer qu'alors les primitives de f sont paires.
2. Si f est paire, montrer qu'alors f possède une seule primitive impaire.

10.21. Soit f la fonction définie sur \mathbb{R}_+ par $f(x) = \int_1^{2x+1} \frac{1}{t} \, dt$. Montrer que f est dérivable puis calculer f' .

10.22. Soit f la fonction définie sur \mathbb{R}_+ par $f(x) = \int_x^{2x} e^{-t^2} \, dt$. Montrer que f est dérivable puis calculer f' .

10.23. On définit, pour $n \geq 1$, $I_n = \int_0^1 t^n e^{-t} \, dt$.

1. Montrer, sans calculer I_n , que la suite (I_n) est décroissante. Converge-t-elle ?
2. Montrer que $0 \leq I_n \leq \frac{1}{n+1}$ et en déduire la limite de (I_n) .

10.24. 1. Si $n \in \mathbb{N}^*$, montrer que $\int_n^{n+1} \frac{1}{x} \, dx < \frac{1}{n}$.

2. En déduire que $\int_1^N \frac{1}{x} \, dx < \frac{1}{1} + \frac{1}{2} + \dots + \frac{1}{N-1}$, où $N \in \mathbb{N}^*$.

3. Que vaut la somme infinie $\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \dots$?

10.25. On considère un courant sinusoïdal d'intensité $i(t) = I_m \sin \omega t$. L'intensité efficace I_e est l'intensité d'un courant continu qui dissiperait dans une résistance la même énergie que $i(t)$ sur une période, i.e. $R I_e^2 T = \int_0^T R i(t)^2 \, dt$. Montrer que $I_e = \frac{I_m}{\sqrt{2}}$.

Intégration par parties

10.26. Calculer une primitive de xe^x sur \mathbb{R} .

10.27. Calculer les intégrales suivantes :

1. $\int_0^1 xe^{2x} dx$;
2. $\int_0^\pi x \sin x dx$;
3. $\int_{-\pi}^\pi x \cos x dx$.

10.28. Calculer les intégrales suivantes :

1. $\int_1^e \ln x dx$;
2. $\int_1^e x \ln x dx$.

10.29. Calculer les intégrales suivantes en intégrant deux fois par parties :

1. $\int_0^1 x^2 e^{-x} dx$;
2. $\int_0^{\frac{\pi}{4}} e^x \cos x dx$.

10.30. Calculer conjointement $I = \int_0^{\frac{\pi}{2}} x \cos^2 x dx$ et $J = \int_0^{\frac{\pi}{2}} x \sin^2 x dx$.

10.31. Soit $I_n = \int_0^1 x^n e^x dx$, où $n \in \mathbb{N}$.

1. Montrer que $I_n = e - nI_{n-1}$.
2. En déduire I_3 .

10.32. Les *coefficients de Fourier* d'une fonction T -périodique f de classe C^1 (i.e. dérivable dont la dérivée est continue) sont définis par $a_n = \frac{2}{T} \int_0^T f(t) \cos \omega n t dt$ et $b_n = \frac{2}{T} \int_0^T f(t) \sin \omega n t dt$, pour $n \geq 1$. Montrer, en intégrant par parties, que ces coefficients tendent vers 0 lorsque n tend vers $+\infty$ (*lemme de Riemann-Lebesgue*).

Calcul d'aires, de volumes et de centres d'inerties

10.33. Calculer l'aire comprise entre la courbe de la fonction cube et l'axe des abscisses entre -1 et 1 .

10.34. Calculer l'aire du domaine fermé délimité par les courbes des fonctions carré et racine carrée.

10.35. Calculer l'aire du domaine fermé délimité par les paraboles d'équations $y = -x^2 + 3x + 16$ et $y = x^2 + 3x - 16$.

10.36. Calculer l'aire comprise entre la courbe du \ln et l'axe des abscisses entre e^{-1} et e .

10.37. Le volume d'un solide est donné par la somme des aires des sections de ce solide par des plans parallèles. Par exemple, imaginer que l'on coupe un saucisson en tranches ; pour le reconstituer, on rassemble toutes les tranches.

1. On considère le cylindre d'équation $x^2 + y^2 = 1$.

Calculer le volume intérieur du cylindre compris entre $z = 1$ et $z = 4$.

2. On considère la boule de centre O et de rayon r , dont on cherche le volume V .

(a) Montrer que $V = 2 \int_0^r \pi(r^2 - z^2) dz$.

(b) En déduire V .

On pourra remarquer que la dérivée du volume d'une boule donne sa surface et que la dérivée de l'aire d'un disque donne son périmètre. Un hasard sans doute...

3. On considère le cône plein d'équation $x^2 + y^2 \leq z^2$.

(a) Montrer que l'aire d'une section horizontale de ce cône vaut πz^2 .

(b) En déduire le volume du cône entre $z = 0$ et $z = 2$.

10.38. On considère une plaque homogène P d'aire A possédant un axe de symétrie. La position de son centre d'inertie sur cet axe, disons repéré par x , est donnée par la moyenne pondérée m_x des valeurs x par les aires $f(x)dx$ des plaques rectangulaires infinitésimales correspondantes. Ainsi l'on obtient $m_x = \frac{1}{A} \int_{P_x} x f(x) dx$.

Déterminer le centre d'inertie de la plaque homogène délimitée par la parabole d'équation $x = y^2$ et la droite d'équation $x = 1$.

Méthodes numériques

10.39 (méthodes des rectangles et des trapèzes). Soit f une fonction continue, positive et croissante sur un intervalle $I = [a; b]$. On subdivise I en n parties égales. On note s_n et S_n les sommes sur I des aires des *rectangles* inférieurs et supérieurs respectivement, et T_n la somme des aires des *trapèzes* naturellement construits à partir de la subdivision. (Sous GeoGebra, les commandes sont `SommeInférieure[f,a,b,n]`, `SommeSupérieure[f,a,b,n]` et `SommeTrapèzes[f,a,b,n]`.)

1. Vérifier que $T_n = \frac{s_n + S_n}{2}$ et en particulier que $s_n \leq T_n \leq S_n$.

2. Montrer que $s_n \leq \int_a^b f \leq S_n$.

3. Évaluer $S_n - s_n$ puis donner une majoration de l'erreur ici commise par la méthode des trapèzes.

4. Montrer que T_n tend vers $\int_a^b f$.

- Une méthode est d'ordre k lorsque l'erreur commise est majorée par une quantité du type $\frac{C}{n^k}$. La méthode des trapèzes est d'ordre 2 ; nous ne venons de montrer qu'une convergence d'ordre 1, à l'image de la méthode des rectangles.
- Attention, les suites (s_n) et (S_n) ne sont pas toujours adjacentes, même si c'est souvent le cas.

- La méthode des rectangles peut éclairer la notion de valeur moyenne de la manière suivante. On échantillonne la fonction f aux abscisses $x_k = a + k \frac{b-a}{n}$ ($k = 0, \dots, n-1$) et on calcule la moyenne des valeurs prises par f sur ces abscisses :

$$\tilde{\mu}_n = \frac{1}{n}(f(x_0) + \dots + f(x_{n-1})) = \frac{1}{b-a} \left(\frac{b-a}{n} f(x_0) + \dots + \frac{b-a}{n} f(x_{n-1}) \right).$$

Cette moyenne n'est qu'une somme d'aires de rectangles et tend donc vers $\frac{1}{b-a} \int_a^b f$, ce qui justifie encore la définition de μ .

10.40. Soit f la fonction définie sur \mathbb{R}_+ par $f(x) = \frac{1}{1+x}$.

Soit (u_n) la suite de terme général $u_n = \frac{1}{n+1} + \frac{1}{n+2} + \dots + \frac{1}{n+n}$.

1. Montrer que $u_n = \frac{1}{n} \left(f\left(\frac{1}{n}\right) + f\left(\frac{2}{n}\right) + \dots + f\left(\frac{n}{n}\right) \right)$.
2. En reconnaissant une valeur moyenne, calculer la limite de la suite (u_n) .

10.41 (méthode de Monte-Carlo). Soit f une fonction continue et positive sur un intervalle $I = [a; b]$. Notons M le maximum de f sur I . On tire un point au hasard uniforme dans le rectangle $I \times [0; M]$. Lorsque ce point est situé sous la courbe, on compte 1 ; sinon on compte 0 (méthode du rejet). On répète n fois cette expérience aléatoire et on note S_n la somme obtenue.

1. Expliquer, en invoquant la loi des grands nombres, pourquoi $\frac{S_n}{n}$ tend vers $\frac{\int_a^b f}{M(b-a)}$.
2. En déduire une approximation de $\int_a^b f$.

On reviendra, lors de l'étude de la loi normale, sur la qualité de cette approximation.

10.42. Mettre en oeuvre les algorithmes des trois méthodes numériques étudiées pour :

1. la fonction carré sur $[0; 1]$;
2. la gaussienne $\frac{1}{\sqrt{2\pi}} e^{-x^2/2}$ sur $[-1; 1]$, $[-2; 2]$ et $[-3; 3]$

La gaussienne est une fonction ne possédant pas de primitive s'écrivant avec des fonctions usuelles.

11. Produit scalaire

11.1 Expressions du produit scalaire

En pensant à $2xy = (x + y)^2 - x^2 - y^2$ on est amené à la définition suivante du produit de deux vecteurs :

Définition. Le *produit scalaire* de deux vecteurs \vec{u} et \vec{v} est le nombre réel donné par l'identité de *polarisation* :

$$\vec{u} \cdot \vec{v} = \frac{1}{2} (\|\vec{u} + \vec{v}\|^2 - \|\vec{u}\|^2 - \|\vec{v}\|^2).$$

Remarque. • On rencontre aussi les notations $\langle \vec{u}, \vec{v} \rangle$ ou $\langle \vec{u} | \vec{v} \rangle$.

- Cette définition est identique à celle donnée dans le plan.

Théorème. On dispose d'autres expressions du produit scalaire :

- dans un repère *orthonormal*, le produit scalaire de $\vec{u}(x; y; z)$ et $\vec{v}(x'; y'; z')$ est donné par :

$$\vec{u} \cdot \vec{v} = xx' + yy' + zz' \quad ;$$

- si \vec{u} et \vec{v} sont non nuls, leur produit scalaire est donné par :

$$\vec{u} \cdot \vec{v} = \|\vec{u}\| \|\vec{v}\| \cos(\widehat{(\vec{u}, \vec{v})}) \quad ;$$

- si $\vec{u} = \overrightarrow{AB}$ et $\vec{v} = \overrightarrow{AC}$, et si H est le projeté orthogonal de C sur (AB) , alors :

$$\vec{u} \cdot \vec{v} = \pm AB \cdot AH, \text{ le signe étant positif si } \overrightarrow{AH} \text{ et } \overrightarrow{AB} \text{ ont même sens, négatif sinon.}$$

Remarque. • Toutes les propriétés du produit scalaire plan sont conservées ; la plupart du temps, les preuves de ces propriétés peuvent se faire en choisissant un repère orthonormal et en appliquant l'expression du produit scalaire avec les coordonnées.

- Attention, l'espace ne peut être muni d'une orientation des angles : l'angle orienté (\vec{u}, \vec{v}) n'existe donc pas, au contraire de l'angle géométrique $(\widehat{(\vec{u}, \vec{v})})$. De toute façon, le cosinus étant pair, un éventuel signe n'importe pas.

Théorème (orthogonalité). $\vec{u} \cdot \vec{v} = 0 \Leftrightarrow \vec{u} = \vec{0}$ ou $\vec{v} = \vec{0}$ ou $\vec{u} \perp \vec{v}$.

Preuve. C'est une conséquence directe de l'expression du produit scalaire avec le cosinus. \square

Définition. Deux droites de vecteurs directeurs \vec{u} et \vec{v} sont *orthogonales* si $\vec{u} \perp \vec{v}$.

11.2 Plans

11.2.1 Généralités

Définition. Un *plan* \mathcal{P} est l'ensemble des points M engendré par un repère $(A; \vec{u}, \vec{v})$, i.e. :

$$M \in \mathcal{P} \Leftrightarrow \exists \lambda, \mu \in \mathbb{R}, \overrightarrow{AM} = \lambda \vec{u} + \mu \vec{v}.$$

Définition. Une droite est *orthogonale* à un plan si elle est orthogonale à toute droite du plan.

Théorème. Une droite est orthogonale au plan \mathcal{P} ssi elle est orthogonale à deux droites sécantes de \mathcal{P} .

Preuve. Soit \vec{n} un vecteur directeur d'une droite \mathcal{D} orthogonale à deux droites sécantes \mathcal{D}_1 et \mathcal{D}_2 de \mathcal{P} , possédant deux vecteurs directeurs \vec{u} et \vec{v} non colinéaires. Donnons-nous une autre droite \mathcal{D}_3 quelconque de \mathcal{P} , de vecteur directeur \vec{w} . On a $\vec{w} = \lambda\vec{u} + \mu\vec{v}$ car $(\vec{u}; \vec{v})$ est une base de \mathcal{P} . Il suit que $\vec{n} \cdot \vec{w} = \vec{n} \cdot (\lambda\vec{u} + \mu\vec{v}) = \lambda\vec{n} \cdot \vec{u} + \mu\vec{n} \cdot \vec{v} = 0 + 0 = 0$ et ainsi $\mathcal{D} \perp \mathcal{D}_3$. \square

Remarque. Ceci signifie donc qu'il suffit de montrer l'orthogonalité de \vec{n} avec une *base* de \mathcal{P} .

Définition. Un vecteur *normal* à un plan \mathcal{P} est un vecteur orthogonal à ce plan.

11.2.2 Équation cartésienne

Dans la suite, on munit l'espace d'un repère orthonormal $(0; \vec{i}, \vec{j}, \vec{k})$.

Théorème. Soient \mathcal{P} un plan, A un point de \mathcal{P} et \vec{n} un vecteur normal à \mathcal{P} . Le plan \mathcal{P} est alors l'ensemble des points M vérifiant $\overrightarrow{AM} \cdot \vec{n} = 0$.

Preuve. Soit (\vec{u}, \vec{v}) une base de \mathcal{P} . On peut vérifier que le vecteur (miraculeusement obtenu par produit vectoriel...) $(y_{\vec{u}z\vec{v}} - y_{\vec{v}z\vec{u}})\vec{i} - (x_{\vec{u}z\vec{v}} - x_{\vec{v}z\vec{u}})\vec{j} + (x_{\vec{u}y\vec{v}} - x_{\vec{v}y\vec{u}})\vec{k}$ est normal à \mathcal{P} , donc il existe un vecteur normal à \mathcal{P} .

- Si M est un point de \mathcal{P} alors par définition il existe $\lambda, \mu \in \mathbb{R}$ tels que $\overrightarrow{AM} = \lambda\vec{u} + \mu\vec{v}$. Il est alors aisé de calculer que $\overrightarrow{AM} \cdot \vec{n} = 0$ car $\vec{u} \cdot \vec{n} = 0$ et $\vec{v} \cdot \vec{n} = 0$.
- Réciproquement, supposons que $\overrightarrow{AM} \cdot \vec{n} = 0$. L'espace possède une base $(\vec{u}, \vec{v}, \vec{n})$ donc $\overrightarrow{AM} = \lambda\vec{u} + \mu\vec{v} + \nu\vec{n}$. En développant $\overrightarrow{AM} \cdot \vec{n} = 0$, il vient $\nu\vec{n}^2 = 0$, ce qui signifie que $\nu = 0$, i.e. $\overrightarrow{AM} = \lambda\vec{u} + \mu\vec{v}$. Par définition, M appartient donc à \mathcal{P} .

\square

Remarque. Un plan peut donc être défini par la donnée d'un point et d'un vecteur normal.

Théorème. • Tout plan \mathcal{P} possède une équation *cartésienne* de la forme $ax + by + cz + d = 0$ où a, b, c ne sont pas tous nuls. Le vecteur $\vec{n}(a; b; c)$ est alors normal à \mathcal{P} .
• Réciproquement, si a, b, c ne sont pas tous nuls alors l'ensemble des points $M(x; y; z)$ vérifiant $ax + by + cz + d = 0$ est un plan de vecteur normal $\vec{n}(a; b; c)$.

Preuve. Soit $A(x_0; y_0; z_0)$ un point de \mathcal{P} . On procède directement par équivalence : $M \in \mathcal{P} \Leftrightarrow \overrightarrow{AM} \cdot \vec{n} = 0 \Leftrightarrow (x - x_0)a + (y - y_0)b + (z - z_0)c = 0 \Leftrightarrow ax + by + cz - (ax_0 + by_0 + cz_0) = 0$ et on pose ensuite $d = -(ax_0 + by_0 + cz_0)$. \square

11.2.3 Distance d'un point à un plan

Lemme. Soient A un point, \vec{n} un vecteur non nul et \mathcal{P} le plan passant par A et orthogonal à \vec{n} . Soient M un point et H son projeté orthogonal sur \mathcal{P} . Alors $MH = \frac{|\overrightarrow{AM} \cdot \vec{n}|}{\|\vec{n}\|}$.

Preuve. Il suffit de projeter A sur (HM) puis de remarquer que $(HM) \parallel \vec{n}$. Il en résulte que $\overrightarrow{AM} \cdot \vec{n} = \overrightarrow{HM} \cdot \vec{n} = \pm HM \cdot \|\vec{n}\|$, d'où l'égalité recherchée. \square

Théorème. La distance entre un point M et son projeté orthogonal H sur le plan \mathcal{P} est la distance minimale de M à un point de \mathcal{P} . C'est la *distance* de M à \mathcal{P} , notée $d(M, \mathcal{P})$.

Preuve. Si K est un autre point de \mathcal{P} que H , alors le théorème de Pythagore prouve que $MK > MH$. \square

Théorème (distance d'un point à un plan). Soit \mathcal{P} le plan d'équation $ax + by + cz + d = 0$ et soit $M(x_0; y_0; z_0)$ un point. Alors :

$$d(M, \mathcal{P}) = \frac{|ax_0 + by_0 + cz_0 + d|}{\sqrt{a^2 + b^2 + c^2}}.$$

Preuve. Soit $A(x_A; y_A; z_A)$ un point de \mathcal{P} ; on a donc $ax_A + by_A + cz_A = -d$. On applique le théorème précédent et la formule du lemme : $d(M, \mathcal{P}) = MH = \frac{|\overrightarrow{AM} \cdot \vec{n}|}{\|\vec{n}\|}$. En passant aux coordonnées : $d(M, \mathcal{P}) = \frac{|(x_0 - x_A)a + (y_0 - y_A)b + (z_0 - z_A)c|}{\sqrt{a^2 + b^2 + c^2}}$. On simplifie ensuite : $d(M, \mathcal{P}) = \frac{|ax_0 + by_0 + cz_0 - (ax_A + by_A + cz_A)|}{\sqrt{a^2 + b^2 + c^2}} = \frac{|ax_0 + by_0 + cz_0 - (-d)|}{\sqrt{a^2 + b^2 + c^2}}$ d'où la formule recherchée. \square

Remarque. Cette formule exprime le *potentiel* du point M par rapport au plan \mathcal{P} , la fonction potentiel étant $f(x, y, z) = |ax + by + cz + d|$, qui doit être normalisée pour compenser le *choix* du vecteur normal utilisé. Plus $M(x, y, z)$ s'éloigne de \mathcal{P} , plus $f(x, y, z)$ augmente.

11.2.4 Demi-espaces

Théorème. Le plan \mathcal{P} d'équation $ax + by + cz + d = 0$ partage l'espace en deux *demi-espaces* :

- l'ensemble des points M tels que $ax + by + cz + d > 0$;
- l'ensemble des points M tels que $ax + by + cz + d < 0$.

Preuve. Soit $\vec{n}(a; b; c)$ le vecteur normal canoniquement associé à l'équation de \mathcal{P} . On prend un point A quelconque dans \mathcal{P} . Le produit scalaire $\overrightarrow{AM} \cdot \vec{n}$, par le théorème de projection, est positif si M est du demi-espace défini par \mathcal{P} et pointé par \vec{n} , négatif sinon. L'expression de ce produit scalaire conduit, comme nous l'avons déjà vu, à l'équation cartésienne de \mathcal{P} ici utilisée. \square

Remarque. Attention cependant, la positivité n'est pas donnée par le sens du vecteur normal !

11.3 Exercices

Généralités

11.1. Soit $ABCD$ un tétraèdre régulier d'arête a . Calculer $\overrightarrow{AB} \cdot \overrightarrow{AC}$.

11.2. Soit $ABCDEFGH$ un cube d'arête a . Calculer $\overrightarrow{AE} \cdot \overrightarrow{AF}$, $\overrightarrow{AE} \cdot \overrightarrow{AG}$ et $\overrightarrow{AF} \cdot \overrightarrow{HC}$.

11.3. On se place dans une repère orthonormal. Soient $A(-7; 12; -20)$, $B(-3; 15; -55)$, $C(20; 1; 0)$ et $D(-8; -20; -5)$. Montrer que $(AB) \perp (CD)$, que ACD est équilatéral, que CBD est isocèle et retrouver que $(AB) \perp (CD)$.

11.4. On se place dans un repère orthonormal. Soient $A(-1; 1; 2)$, $B(0; 1; 0)$ et $C(2; 0; 3)$. Calculer une mesure approchée de l'angle \widehat{BAC} .

11.5 (théorème du toit). Soient deux plans sécants contenant deux droites parallèles. Montrer que la droite d'intersection des deux plans est parallèle aux deux droites.

Configurations

11.6. Soit $ABCDEFGH$ un cube. Montrer que $(AG) \perp (FCH)$.

11.7. Soit $ABCD$ un tétraèdre régulier. Soient I le milieu de $[AD]$ et J celui de $[BC]$. Montrer que la droite (IJ) est orthogonale aux arêtes qui portent I et J .

11.8. Soit $ABCDEFGH$ un parallélépipède rectangle vérifiant $AB = AE = 2$ et $AD = 4$. Soient I le centre de la face $ABFE$ et J le milieu de l'arête $[EH]$. Déterminer une mesure approchée de l'angle \widehat{IJG} .

11.9. Soit $SABCD$ une pyramide régulière à base carrée de côté a , de hauteur h . Montrer que $\overrightarrow{SA} \cdot \overrightarrow{SC} = h^2 - \frac{a^2}{2}$.

11.10. On considère un cube $ABCDEFGH$ de côté 1, avec E au-dessus de A . On note I le milieu de $[BC]$, J celui de $[EH]$ et Ω le centre de la face $CDHG$.

1. Montrer que A, I, G et J sont coplanaires.
2. Montrer que $\overrightarrow{IJ} = \overrightarrow{CH}$ et en déduire que $\overrightarrow{F\Omega} \cdot \overrightarrow{IJ} = 0$.
3. Montrer que la droite $(F\Omega)$ est orthogonale au plan $(AIGJ)$.

11.11. Soit $ABCD$ un tétraèdre régulier d'arête a et soit O son *centre* (i.e. l'isobarycentre de ses sommets).

1. Montrer que deux arêtes opposées sont orthogonales.
2. Soit A' le centre de la face BCD .
 - (a) Montrer que O appartient à la *médiane* $[AA']$.
 - (b) Exprimer \overrightarrow{AO} en fonction de $\overrightarrow{AA'}$.

- (c) Montrer que $\overrightarrow{AB} + \overrightarrow{AC} + \overrightarrow{AD} = 3\overrightarrow{AA'}$.
- (d) En déduire que les médianes du tétraèdre régulier sont aussi les hauteurs.
3. (a) Montrer que le plan médiateur de $[AB]$ est (ICD) où I est le milieu de $[AB]$.
- (b) Montrer que O appartient à (ICD) .
- (c) En déduire que O est aussi le centre de la sphère circonscrite au tétraèdre régulier.

Droites et plans

Dans cette section, on munit l'espace d'un repère orthonormal.

11.12. Déterminer un vecteur normal au plan d'équation $31x + 37y + 41z + 43 = 0$.

11.13. Le vecteur $\vec{n}(6; -2; 4)$ est-il normal au plan d'équation $-3x + y - 3z = 1$?

11.14. Déterminer une équation cartésienne du plan contenant $A(2; -1; 1)$ et orthogonal au vecteur $\vec{n}(3; -4; 2)$

11.15. Déterminer une équation cartésienne du plan \mathcal{P} passant par $A(-2; 1; 3)$ et orthogonal à (BC) où $B(1; -2; 2)$ et $C(4; 1; -1)$.

11.16. Soient $A(-2; 3; 5)$ et $B(4; -1; 3)$. Déterminer une équation cartésienne du plan médiateur du segment $[AB]$.

11.17. Les plans $\mathcal{P} : 2x - y + z + 9 = 0$ et $\mathcal{Q} : x + y - z - 7 = 0$ sont-ils orthogonaux?

11.18. Les plans \mathcal{P} et \mathcal{Q} suivants sont-ils confondus? parallèles? sécants? orthogonaux?

1. $\mathcal{P} : x - 4y + 7 = 0$ et $\mathcal{Q} : x + 2y - z + 1 = 0$;

2. $\mathcal{P} : x - 2y + 3z - 1 = 0$ et $\mathcal{Q} : 2x - 4y + 6z = 0$;

3. $\mathcal{P} : 2x + y - z + 1 = 0$ et $\mathcal{Q} : x + 2y + 4z - 5 = 0$.

11.19. Soient $A(1; -1; 1)$, $B(0; 2; -1)$ et $C(-1; 1; 0)$. Montrer que A , B et C forment un plan puis déterminer x afin que $\vec{u}(x; 3; 4)$ soit normal à (ABC) .

11.20. Soient $\mathcal{P} : 2x - y + z + 9 = 0$ et $\mathcal{Q} : x + y + 2z - 7 = 0$. Calculer l'angle aigu formé par ces deux plans.

11.21. Calculer la distance du point $M(5; 2; -3)$ au plan d'équation $x + 4y + 8z = -2$.

11.22. Soit \mathcal{D} la droite passant par $A(1; -1; 2)$ et de vecteur directeur $\vec{u}(2; 2; 1)$. Déterminer la distance de $M(2; -5; 3)$ à \mathcal{D} .

11.23. Soient $A(1; 0; 2)$, $B(2; -3; 1)$ et $C(0; 1; -2)$. Calculer la hauteur AH du triangle ABC .

11.24. Les points $A(1; 1; 1)$ et $B(-4; 3; 1)$ sont-ils dans le même demi-espace défini par $\mathcal{P} : 2x - y + z + 9 = 0$?

11.25. Représenter la région de l'espace définie par $x + y + z \leq 1$ et $x, y, z \geq 0$.

11.26. Soient $A(a; 0; 0)$, $B(0; b; 0)$ et $C(0; 0; c)$ avec $a, b, c > 0$.

1. Déterminer une équation du plan (ABC) en cherchant un vecteur normal.

2. Montrer que si $h = d(O, (ABC))$ alors $\frac{1}{h^2} = \frac{1}{a^2} + \frac{1}{b^2} + \frac{1}{c^2}$.

12. Droites et plans

12.1 Barycentres

Théorème (définition du barycentre). Soit $\{(A_1, \alpha_1), \dots, (A_n, \alpha_n)\}$ un ensemble (ou *système*) de points pondérés vérifiant $\alpha_1 + \dots + \alpha_n \neq 0$. Le *barycentre* de ce système de points est l'unique point G vérifiant $\alpha_1 \overrightarrow{GA_1} + \dots + \alpha_n \overrightarrow{GA_n} = \vec{0}$.

Remarque. • Le point G est donc la « moyenne pondérée » des points (A_i, α_i) .

- Ses coordonnées se calculent en faisant la moyenne pondérée de celles des points (A_i, α_i) .
- On peut effectuer la *réduction vectorielle* $\alpha_1 \overrightarrow{MA_1} + \dots + \alpha_n \overrightarrow{MA_n} = (\alpha_1 + \dots + \alpha_n) \overrightarrow{MG}$.

Théorème (associativité). Soit $\mathcal{S} = \{(A_1, \alpha_1), \dots, (A_n, \alpha_n)\}$ un système de points pondérés vérifiant $\alpha_1 + \dots + \alpha_n \neq 0$. Le barycentre de ce système peut être obtenu en partitionnant \mathcal{S} par des sous-ensembles de poids non nuls, en déterminant leurs barycentres (barycentres *partiels* de \mathcal{S}) puis en calculant le barycentre de ces barycentres partiels.

12.2 Plans

Dans cette section, on munit l'espace d'un repère orthonormal.

Définition. Deux plans \mathcal{P} et \mathcal{P}' de vecteurs normaux \vec{n} et \vec{n}' sont :

- *parallèles* si \vec{n} et \vec{n}' sont colinéaires ;
- *orthogonaux* si \vec{n} et \vec{n}' sont orthogonaux.

Remarque. Si \mathcal{P} et \mathcal{P}' sont orthogonaux et si A est un point de leur intersection alors la droite passant par A et dirigée par \vec{n} (resp. \vec{n}') est contenue dans \mathcal{P}' (resp. \mathcal{P}).

Définition. Soient A un point d'un plan \mathcal{P} et (\vec{u}, \vec{v}) une base de \mathcal{P} . Alors $(A; \vec{u}, \vec{v})$ est un repère de \mathcal{P} et définit une *équation paramétrique* de \mathcal{P} par :

$$M(x; y; z) \in \mathcal{P} \Leftrightarrow \exists s, t \in \mathbb{R}, \overrightarrow{AM} = s\vec{u} + t\vec{v} \Leftrightarrow \exists s, t \in \mathbb{R}, \begin{cases} x = x_A + sx_{\vec{u}} + tx_{\vec{v}} \\ y = y_A + sy_{\vec{u}} + ty_{\vec{v}} \\ z = z_A + sz_{\vec{u}} + tz_{\vec{v}} \end{cases}.$$

Remarque. • L'égalité vectorielle étant très facile à retenir, il faut noter qu'elle donne par simple passage aux coordonnées le système paramétrique.

- Il y a une infinité de paramétrisations possibles pour un même plan ; déterminer leur équivalence n'est pas trivial, contrairement aux équations cartésiennes (qui sont proportionnelles entre elles).
- On peut donc définir analytiquement un plan de deux façons : par équation cartésienne ou par équation paramétrique. Le passage d'une forme à l'autre n'est pas trivial, d'autant que nous ne disposons pas du produit vectoriel...

12.3 Droites

Dans cette section, on munit l'espace d'un repère orthonormal.

Définition. Soient A un point d'une droite \mathcal{D} . Soit \vec{u} un vecteur directeur de \mathcal{D} ; $(A; \vec{u})$ est alors un repère de \mathcal{D} , qui définit une *équation paramétrique* de \mathcal{D} par :

$$M(x; y; z) \in \mathcal{D} \Leftrightarrow \exists t \in \mathbb{R}, \overrightarrow{AM} = t\vec{u} \Leftrightarrow \exists t \in \mathbb{R}, \begin{cases} x = x_A + tx_{\vec{u}} \\ y = y_A + ty_{\vec{u}} \\ z = z_A + tz_{\vec{u}} \end{cases}.$$

Remarque. • Comme pour les plans, le système paramétrique est facile à retenir.

- Il n'y a pas d'équation cartésienne de droite dans l'espace : schématiquement, une équation fixe une dimension, or il faut dans l'espace (de dimension 3) en enlever deux pour obtenir une droite (de dimension 1).
- On peut par contre définir une droite comme intersection de deux plans ; le passage de ce système à une équation paramétrique n'est pas trivial.

12.4 Intersections

Théorème. L'intersection de deux droites peut donner :

- l'ensemble vide ;
- un point ;
- ces droites confondues.

Théorème. L'intersection d'une droite et d'un plan peut donner :

- l'ensemble vide ;
- un point ;
- cette droite, incluse dans le plan.

Théorème. L'intersection de deux plans peut donner :

- l'ensemble vide ;
- une droite ;
- ces plans confondus.

Théorème. L'intersection de trois plans peut donner :

- l'ensemble vide (sans qu'ils soient nécessairement parallèles) ;
- un point ;
- une droite ;
- ces plans confondus.

12.5 Exercices

Barycentres

12.1. Montrer sans calcul que le centre d'inertie (isobarycentre) d'un triangle est situé aux deux tiers des médianes.

12.2. Soit ABC un triangle.

1. Montrer que le point M défini par $\overrightarrow{AM} = \frac{2}{5}\overrightarrow{AB} + \frac{3}{5}\overrightarrow{AC}$ est un barycentre de B et C .
2. Les points B , C et M sont-ils alignés ?

12.3. Soient A , B et C trois points non alignés. Montrer que l'ensemble des points M vérifiant $\|3\overrightarrow{MA} + \overrightarrow{MB}\| = 2\|\overrightarrow{MA} + \overrightarrow{MC}\|$ forme un plan que l'on précisera.

12.4. Soient $A(6; 0; 0)$ et $B(0; 6; 0)$.

1. Déterminer le barycentre G du système de points $\{(O, 1), (A, 2), (B, 3)\}$.
2. Soit $C(0; 0; 4)$ et soit \mathcal{S} l'ensemble des points $M(x; y; z)$ vérifiant l'équation vectorielle $(\overrightarrow{MO} + 2\overrightarrow{MA} + 3\overrightarrow{MB}) \cdot \overrightarrow{MC} = 0$. Déterminer avec et sans coordonnées l'ensemble \mathcal{S} .
3. Déterminer l'intersection de \mathcal{S} avec le plan d'équation $x = 0$.

Droites et plans

Dans cette section, on munit l'espace d'un repère orthonormal.

12.5. Soient $A(-1; 2; -3)$ et $B(1; -1; 1)$. Déterminer une représentation paramétrique de la droite (AB) .

12.6. Vérifier que $\vec{u}(1; -1; 2)$ et $\vec{v}(-1; -2; 1)$ ne sont pas colinéaires puis donner une représentation paramétrique du plan contenant $A(2; 1; -1)$ et dirigé par (\vec{u}, \vec{v}) .

12.7. Donner l'équation cartésienne du plan contenant $A(-1; 1; 1)$ et parallèle au plan d'équation $3x - y + z - 5 = 0$.

12.8. Déterminer une équation paramétrique du plan contenant $A(7; -5; -4)$ et parallèle au plan d'équation paramétrique :

$$\begin{cases} x = t - 1 \\ y = 2t - u + 1 \\ z = 2u + 3 \end{cases} .$$

12.9. La droite \mathcal{D} dont une représentation paramétrique est :

$$\begin{cases} x = 1 - t\sqrt{2} \\ y = 2t - 1 \\ z = t\sqrt{2} - 1 \end{cases}$$

est-elle contenue dans le plan \mathcal{P} d'équation $3x + \sqrt{2}y + z - 2 + \sqrt{2} = 0$?

12.10. Les équations paramétriques :

$$\begin{cases} x = -1 + 2t \\ y = 2 - 3t \\ z = -3 + 4t \end{cases} \quad \text{et} \quad \begin{cases} x = 1 - 4t \\ y = -1 + 6t \\ z = 1 - 8t \end{cases}$$

définissent-elles la même droite ?

12.11. Soient $A(2; -1; 3)$, $B(3; 1; 0)$, $C(0; 2; 5)$ et $D(1; 2; 3)$.

1. Déterminer une équation paramétrique du plan (ABC) .
2. Les points A , B , C et D sont-ils coplanaires ?

12.12. Soient $A(1; 0; -1)$, $B(4; -1; 1)$ et $C(0; 1; 0)$.

1. Déterminer une équation paramétrique de (ABC) puis en déduire une équation cartésienne.
2. Déterminer directement une équation cartésienne de (ABC) .

Les SI pourront vérifier le résultat grâce au produit vectoriel...

12.13. Soient $A(-1; 0; 1)$, $\vec{u}(1; 2; -1)$ et $\vec{v}(3; -1; 2)$. Montrer que $(A; \vec{u}, \vec{v})$ définit un plan dont on déterminera une équation cartésienne.

12.14. Montrer que la droite d'équation paramétrique :

$$\begin{cases} x = -1 + 2t \\ y = 2 - 3t \\ z = -3 + 4t \end{cases}$$

est parallèle au plan d'équation cartésienne $x + 2y + z = 3$.

Intersections

Dans cette section, on munit l'espace d'un repère orthonormal.

12.15. Déterminer le point d'intersection du plan $\mathcal{P} : x + 2y - z + 2 = 0$ et de la droite \mathcal{D} passant par $A(2; 1; -4)$ et dirigée par $\vec{u}(3; -2; 4)$.

12.16. Soit \mathcal{D} la droite passant par $A(2; 0; 0)$ et dirigée par $\vec{u}(0; 1; 1)$. Soit \mathcal{D}' la droite passant par $B(3; 2; 6)$ et dirigée par $\vec{u}'(1; -2; 2)$. Montrer que \mathcal{D} et \mathcal{D}' sont sécantes en trouvant leur point d'intersection. Sont-elles coplanaires ?

12.17. Déterminer une équation paramétrique de la droite d'intersection des deux plans d'équations $2x + y - z - 2 = 0$ et $x + 3y + 7z - 11 = 0$.

12.18. Déterminer une équation paramétrique de la droite d'intersection des deux plans d'équations $3x - y + 2z - 1 = 0$ et $x + 5y - z - 2 = 0$.

12.19. Déterminer l'intersection des trois plans d'équations $2x + 3y - 2z = 2$, $4x - 3y + z = 4$ et $2x + 12y - 7z = 2$.

12.20. Soient $A(1; -1; 2)$ et $B(2; 1; -1)$. Montrer que (AB) est sécante avec la droite Δ , intersection des plans d'équations $2x + y - z - 6 = 0$ et $3x - 2y + z - 3 = 0$.

13. Lois de probabilité

13.1 Loi binomiale

13.1.1 Coefficients binomiaux

Définition. Soit E un ensemble à n éléments.

- Une *combinaison* de E à p éléments est une partie de E à p éléments ;
- le nombre de telles combinaisons est le *coefficient binomial* $\binom{n}{p}$ (se lit « binomial n p » ou « p parmi n »).

Remarque. En particulier, $\binom{n}{1} = n$ et $\binom{n}{0} = \binom{n}{n} = 1$.

Théorème. Soient n et p des entiers positifs vérifiant $0 \leq p \leq n$. Alors :

$$\binom{n}{p} = \frac{n(n-1) \cdots (n-p+1)}{p!} = \frac{n!}{p!(n-p)!}.$$

Preuve. Le nombre de listes à p éléments deux à deux distincts vaut $\binom{n}{p} p!$ (choix des p éléments puis permutations). Ainsi $\binom{n}{p} p! = \frac{n!}{(n-p)!}$, d'où la formule recherchée. \square

13.1.2 Formule du binôme

Théorème (formule du binôme). Soient a et b deux nombres (réels ou complexes). Alors :

$$(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k = a^n + \binom{n}{1} a^{n-1} b + \binom{n}{2} a^{n-2} b^2 + \cdots + \binom{n}{n-1} a b^{n-1} + b^n.$$

Preuve. On a trivialement $(a+b)^n = \overbrace{(a+b)(a+b) \cdots (a+b)}^{n \text{ facteurs}}$. Lors du développement de cette expression, obtenir un terme en $a^{n-k} b^k$ c'est choisir dans k facteurs parmi n le nombre b . Il y a donc $\binom{n}{k}$ possibilités. \square

Théorème. Les coefficients binomiaux vérifient deux relations fondamentales :

- (*symétrie*) $\binom{n}{p} = \binom{n}{n-p}$;
- (*relation de Pascal*) $\binom{n-1}{p-1} + \binom{n-1}{p} = \binom{n}{p}$.

Preuve. Soit E un ensemble à n éléments.

- Choisir p éléments parmi n revient à rejeter les $n - p$ autres éléments. Il y a donc autant de parties de E à p éléments qu'à $n - p$ éléments.
- Soit $a \in E$ un élément quelconque. Il y a $\binom{n-1}{p}$ parties de E à p éléments qui ne contiennent pas a et $\binom{n-1}{p-1}$ parties de E à p éléments qui contiennent a . Il y a donc $\binom{n-1}{p} + \binom{n-1}{p-1}$ parties de E à p éléments, nombre qui vaut $\binom{n}{p}$ par définition.

□

Corollaire. Ces deux relations permettent de construire facilement le triangle de Pascal :

$n \setminus k$	0	1	2	3	4	5	6
0	1						
1	1	1					
2	1	2	1				
3	1	3	3	1			
4	1	4	6	4	1		
5	1	5	10	10	5	1	
6	1	6	15	20	15	6	1

13.1.3 Loi binomiale

On se place dans un espace probabilisé (Ω, P) .

Loi de Bernoulli

Définition. Une *épreuve de Bernoulli* est une expérience aléatoire possédant deux issues (contraires), *succès* et *échec*, de probabilités p et q (avec $p + q = 1$).

Définition. À la suite d'une épreuve de Bernoulli, une variable aléatoire $X : \Omega \rightarrow \mathbb{R}$ vérifiant $X(\text{succès}) = 1$ et $X(\text{échec}) = 0$ suit la *loi de Bernoulli* de paramètre p , noté $X \sim \mathcal{B}(p)$.

Remarque. En résumé, $P(X = 1) = p$ et $P(X = 0) = q$ avec $p + q = 1$.

Théorème. Si $X \sim \mathcal{B}(p)$ alors :

- son espérance vaut $E(X) = p$;
- sa variance vaut $\sigma^2(X) = \text{Var}(X) = V(X) = pq$.

Preuve. • $E(X) = 1 \cdot p + 0 \cdot q = p$.

- $V(X) = E(X^2) - E(X)^2 = 1^2 \cdot p + 0^2 \cdot q - p^2 = p - p^2 = p(1 - p) = pq$.

□

Schéma de Bernoulli et loi binomiale

Définition. Un *schéma de Bernoulli* est la répétition de n épreuves de Bernoulli indépendantes et de même paramètre.

Définition. Si X_1, \dots, X_n sont des variables aléatoires indépendantes et de même loi $\mathcal{B}(p)$ alors $S_n = X_1 + \dots + X_n$ suit la *loi binomiale* de paramètres n et p , notée $\mathcal{B}(n, p)$.

Remarque. Ainsi, S_n compte le nombre de succès lors de n épreuves de Bernoulli indépendantes.

Lemme. Soient X et Y deux variables aléatoires. Alors :

- $E(X + Y) = E(X) + E(Y)$ et $E(\lambda X) = \lambda E(X)$;
- $V(X + Y) = V(X) + V(Y)$ si X et Y sont indépendantes.

Preuve. • On montre directement la linéarité de l'espérance :

$E(X+Y) = \sum_{\omega} (X(\omega) + Y(\omega))P(\{\omega\}) = \sum_{\omega} X(\omega)P(\{\omega\}) + \sum_{\omega} Y(\omega)P(\{\omega\}) = E(X) + E(Y)$. On procède de même pour la deuxième assertion.

- On remarque d'abord, en supposant que X prend les valeurs x_i et Y les valeurs y_j , que $E(XY) = \sum_{i,j} x_i y_j P(X = x_i, Y = y_j)$. Puisque X et Y sont indépendantes, $P(X = x_i, Y = y_j) = P(X = x_i)P(Y = y_j)$. Il vient donc $E(XY) = \sum_{i,j} x_i y_j P(X = x_i)P(Y = y_j) = \sum_i x_i P(X = x_i) \cdot \sum_j y_j P(Y = y_j) = E(X)E(Y)$.

Finalement $V(X+Y) = E((X+Y)^2) - E(X+Y)^2 = E(X^2 + Y^2 + 2XY) - (E(X) + E(Y))^2 = E(X^2) + E(Y^2) + 2E(XY) - E(X)^2 - E(Y)^2 - 2E(X)E(Y) = V(X) + V(Y)$ en utilisant ce que nous venons de montrer.

□

Théorème. Si $X \sim \mathcal{B}(n, p)$ alors :

- $P(X = k) = \binom{n}{k} p^k q^{n-k}$;
- $E(X) = np$;
- $V(X) = npq$ et donc $\sigma(X) = \sqrt{npq}$.

Preuve. • On choisit les emplacements des k succès parmi n épreuves ; il y a $\binom{n}{k}$ choix possibles. Dans chacun de ces k emplacements, la probabilité d'un succès est de p , et dans les $n - k$ autres, la probabilité d'un échec est de q , d'où une probabilité-produit $p^k q^{n-k}$ par indépendance.

- On sait que $X = X_1 + \dots + X_n$ où $X_i \sim \mathcal{B}(p)$. Ainsi $E(X) = E(X_1) + \dots + E(X_n) = p + \dots + p = np$.
- Comme de plus les X_i sont indépendantes, $V(X) = V(X_1) + \dots + V(X_n) = pq + \dots + pq = npq$.

□

Remarque. On vérifie bien que $\sum_{k=0}^n P(S_n = k) = \sum_{k=0}^n \binom{n}{k} p^k q^{n-k} = (p + q)^n = 1^n = 1 \dots$

13.2 Densité

On se place dans un espace probabilisé (Ω, P) .

Définition. Soit X une variable aléatoire sur Ω , prenant ses valeurs sur un intervalle I de bornes $a < b$, avec éventuellement $a = -\infty$ ou $b = +\infty$. La loi P_X de X est à *densité continue* s'il existe une fonction f (la *densité*) définie sur I et vérifiant :

- $f \geq 0$;
- f continue ;
- $\int_a^b f = 1$;
- $P(\alpha \leq X \leq \beta) = \int_\alpha^\beta f$.

Remarque. • La loi P_X ainsi définie est bien une probabilité.

- Si $x_0 \in I$ alors $P_X(x_0) = P(X = x_0) = \int_{x_0}^{x_0} f = 0$ (la loi est *diffuse*). Ainsi une issue peut être réalisable tandis que sa probabilité vaut 0.
- Une conséquence est que l'on ne peut définir la probabilité d'un intervalle comme la somme (intégrale) des probabilités des points qui le composent. On peut par contre interpréter l'aire rectangulaire $f(x)dx$ comme $P(X \in [x; x + dx])$, i.e. la probabilité que X soit dans un voisinage infinitésimal de x . On a alors naturellement $P(\alpha \leq X \leq \beta) = \int_\alpha^\beta P(X \in [x; x + dx])$.

Définition. Soit X une variable aléatoire sur Ω , prenant ses valeurs sur un intervalle I de bornes $a < b$, à densité f sur I .

- $E(X) = \int_a^b x P(X \in [x; x + dx]) = \int_a^b x f(x) dx$ (moyenne des x pondérés) ;
- $V(X) = E((X - E(X))^2) = E(X^2) - E(X)^2 = \int_a^b x^2 f(x) dx - E(X)^2$;
- $F_X(t) = P(X \leq t) = \int_a^t f(x) dx$ pour $a \leq t \leq b$ (*fonction de répartition*).

Théorème. Dans ces conditions :

- les propriétés de l'espérance et de la variance sont les mêmes que dans le cas discret ;
- F_X est une primitive de f .

13.3 Loi uniforme

Définition. La loi uniforme sur $[a; b]$ est la loi $\mathcal{U}([a; b])$ de densité $\frac{1}{b-a}$ sur $[a; b]$.

Théorème. Si $X \sim \mathcal{U}([a; b])$ alors :

- $E(X) = \frac{a+b}{2}$;
- $V(X) = \frac{(b-a)^2}{12}$.

Preuve. • $E(X) = \int_a^b x \frac{1}{b-a} dx = \frac{1}{b-a} \int_a^b x dx = \frac{1}{b-a} \frac{b^2 - a^2}{2} = \frac{a+b}{2}$.

• $V(X) = E(X^2) - E(X)^2 = \int_a^b x^2 \frac{1}{b-a} dx - \left(\frac{a+b}{2}\right)^2 = \frac{1}{b-a} \frac{b^3 - a^3}{3} - \left(\frac{a+b}{2}\right)^2 =$

$$\frac{b^2 + ab + a^2}{3} - \frac{a^2 + 2ab + b^2}{4} = \frac{4b^2 + 4ab + 4a^2}{12} - \frac{3a^2 + 6ab + 3b^2}{12} = \frac{(b-a)^2}{12}.$$

□

13.4 Loi exponentielle

Remarque. L'exercice 13.16 nous a permis de montrer que la durée de vie d'un phénomène sans mémoire, sans usure, sans vieillissement, etc. suit nécessairement une loi à densité bien particulière : une loi exponentielle.

Définition. La *loi exponentielle* de paramètre $\lambda > 0$ est la loi $\mathcal{E}(\lambda)$ de densité $\lambda e^{-\lambda t}$ sur \mathbb{R}_+ .

Théorème. Si $T \sim \mathcal{E}(\lambda)$ alors :

- $P(a \leq T \leq b) = \int_a^b \lambda e^{-\lambda t} dt$;
- $F_T(x) = P(T \leq x) = 1 - e^{-\lambda x}$ (*fonction de répartition*) ;
- $P(T > x) = e^{-\lambda x}$ (*fonction de survie*) ;
- $E(T) = \frac{1}{\lambda}$;
- $V(T) = \frac{1}{\lambda^2}$.

Preuve. • C'est juste la définition d'une densité.

- $F_T(x) = \int_0^x \lambda e^{-\lambda t} dt = [-e^{-\lambda t}]_0^x = 1 - e^{-\lambda x}$.
- $P(T > x) = 1 - P(T \leq x) = 1 - F_T(x) = e^{-\lambda x}$.
- On doit calculer $E(T) = \int_0^{+\infty} t \lambda e^{-\lambda t} dt$. Par définition, $\int_0^{+\infty} f = \lim_{A \rightarrow +\infty} \int_0^A f$ si cette limite existe. On commence donc par intégrer par parties : $\int_0^A t \lambda e^{-\lambda t} dt = [-te^{-\lambda t}]_0^A - \int_0^A -e^{-\lambda t} dt = -Ae^{-\lambda A} - \left[\frac{e^{-\lambda t}}{\lambda} \right]_0^A = -Ae^{-\lambda A} - \frac{e^{-\lambda A}}{\lambda} + \frac{1}{\lambda}$. On fait tendre ensuite A vers $+\infty$, ce qui mène à $E(T) = \frac{1}{\lambda}$.
- On doit ici évaluer $V(T) = \int_0^{+\infty} t^2 \lambda e^{-\lambda t} dt - E(T)^2$. On intègre par parties : $\int_0^A t^2 \lambda e^{-\lambda t} dt = [-t^2 e^{-\lambda t}]_0^A - \int_0^A -2te^{-\lambda t} dt = -A^2 e^{-\lambda A} + \frac{2}{\lambda} E(T)$. On fait tendre ensuite A vers $+\infty$, ce qui mène à $\int_0^{+\infty} t^2 \lambda e^{-\lambda t} dt = \frac{2}{\lambda} E(T)$. Finalement, $V(T) = \frac{2}{\lambda} \frac{1}{\lambda} - \left(\frac{1}{\lambda} \right)^2 = \frac{1}{\lambda^2}$. □

13.5 Loi normale

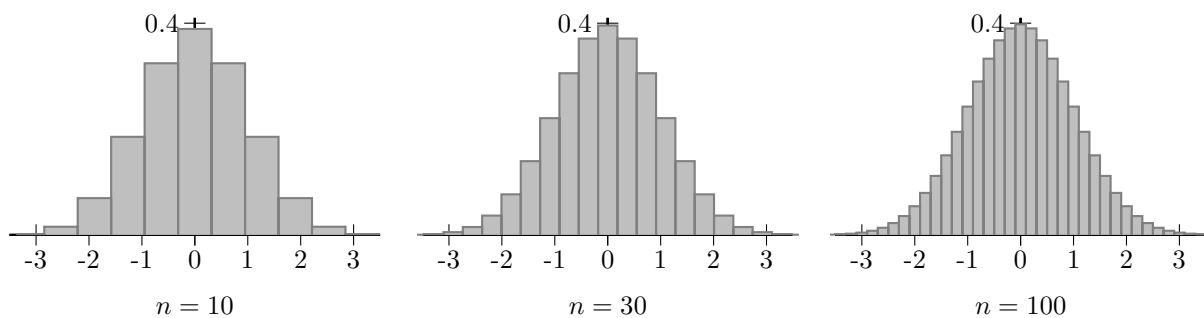
13.5.1 Loi centrée réduite

Théorème (de Moivre-Laplace). Soit $X_n \sim \mathcal{B}(n, p)$ On note $Z_n = \frac{X_n - E(X_n)}{\sigma(X_n)} = \frac{X_n - np}{\sqrt{np(1-p)}}$

la v.a. centrée réduite associée (i.e. $E(Z_n) = 0$ et $\sigma(Z_n) = 1$).

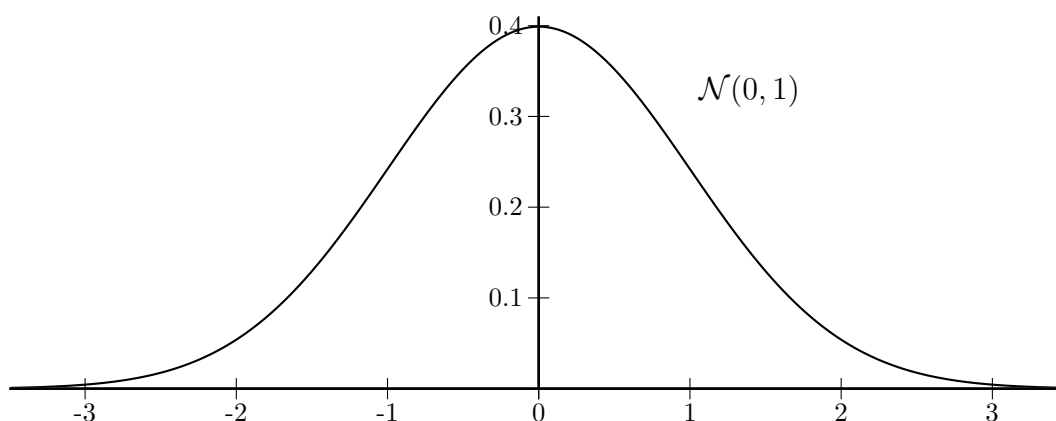
Alors $P(Z_n \in [a; b])$ converge vers $\int_a^b \frac{1}{\sqrt{2\pi}} e^{-x^2/2} dx$.

Preuve. Admise. Visuellement cependant, on peut observer une stabilisation de la densité (dis-
crète) de la suite (Z_n) , ici pour $p = 0,5$:



□

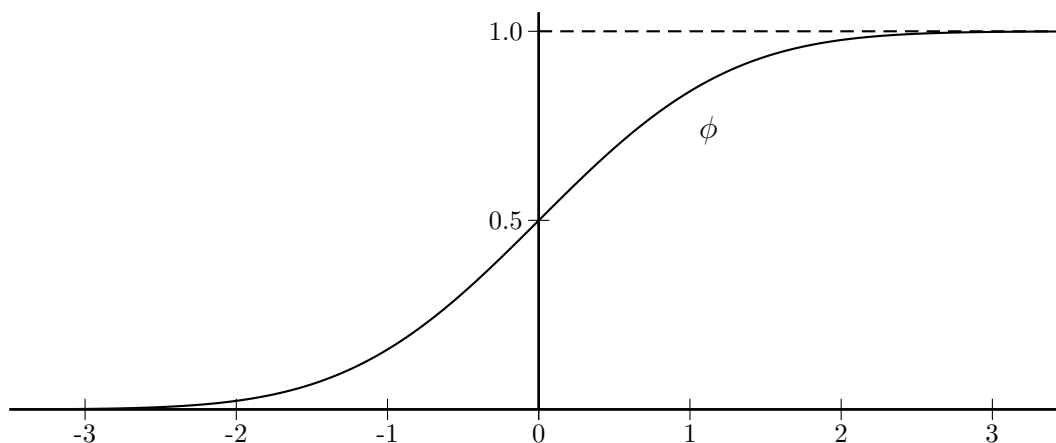
Définition. La loi de densité $\frac{1}{\sqrt{2\pi}}e^{-x^2/2}$ sur \mathbb{R} est la *loi normale centrée réduite* $\mathcal{N}(0, 1)$.



Remarque. • La suite de v.a. (Z_n) converge en loi vers $\mathcal{N}(0, 1)$.

- La densité de la loi $\mathcal{N}(0, 1)$ est paire.
- Par conséquent, si la v.a. X suit la loi $\mathcal{N}(0, 1)$ alors $P(X < 0) = P(X > 0) = \frac{1}{2}$.
- Cette densité ne possède pas de primitive s'écrivant avec des fonctions usuelles.
- Cette densité s'écrase très vite lorsque x s'éloigne de 0.
- La courbe de la densité $\mathcal{N}(0, 1)$ est une *gaussienne*, et la loi $\mathcal{N}(0, 1)$ est fréquemment appelée *gaussienne* ou *loi de Laplace-Gauss*.

Définition. On note ϕ la fonction de répartition de la loi $\mathcal{N}(0, 1)$.



Théorème. Si X suit la loi $\mathcal{N}(0, 1)$, de fonction de répartition ϕ , alors :

- $P(a \leq X \leq b) = \phi(b) - \phi(a)$;
- $\phi(-a) = 1 - \phi(a)$;
- $P(-a \leq X \leq a) = 2\phi(a) - 1$.

Preuve. • Déjà vu : ϕ est simplement une primitive de la densité gaussienne f .

- Si $h(x) = \phi(-x) + \phi(x)$ alors h est dérivable avec $h'(x) = -f(-x) + f(x) = -f(x) + f(x) = 0$ car f est paire. Ainsi h est constante sur \mathbb{R} ; puisque $h(0) = 0,5 + 0,5 = 1$ (toujours par parité de f), il vient $h(x) = 1$ pour tout x .
- On calcule directement : $P(-a \leq X \leq a) = \phi(a) - \phi(-a) = \phi(a) - (1 - \phi(a)) = 2\phi(a) - 1$.

□

Théorème. Si $X \sim \mathcal{N}(0; 1)$ et $\alpha \in]0; 1[$ alors il existe un unique réel u_α vérifiant l'égalité $P(-u_\alpha \leq X \leq u_\alpha) = 1 - \alpha$.

Preuve. L'équation à résoudre est $P(-x \leq X \leq x) = 1 - \alpha$ soit $2\phi(x) - 1 = 1 - \alpha$ ou encore $\phi(x) = 1 - \frac{\alpha}{2}$. La fonction ϕ est continue (car dérivable), strictement croissante (sa dérivée gaussienne étant strictement positive), $\lim_{x \rightarrow -\infty} \phi(x) = 0$ et $\lim_{x \rightarrow +\infty} \phi(x) = 1$. Le théorème des valeurs intermédiaires, puisque $0 < 1 - \frac{\alpha}{2} < 1$, prouve alors l'existence d'un unique u_α vérifiant $\phi(u_\alpha) = 1 - \frac{\alpha}{2}$, i.e. $P(-u_\alpha \leq X \leq u_\alpha) = 1 - \alpha$.

□

Remarque. Avec un logiciel de calcul on obtient les deux résultats à connaître suivants :

- $P(-1,96 \leq X \leq 1,96) \approx 0,95$;
- $P(-2,58 \leq X \leq 2,58) \approx 0,99$.

Remarque. Une v.a. suivant la loi normale a été construite comme limite d'une suite de v.a. d'espérance nulle et de variance égale à 1. Le théorème suivant prouve qu'il en est bien sûr de même pour cette v.a. limite.

Théorème. Soit X une v.a. suivant la loi $\mathcal{N}(0, 1)$. Alors :

- $E(X) = 0$;
- $V(X) = 1$.

Preuve. • Si f est la densité gaussienne, on doit calculer $E(X) = \int_{-\infty}^{+\infty} tf(t)dt$. Par définition, cette intégrale *impropre* vaut $\lim_{x \rightarrow -\infty} \int_x^0 tf(t)dt + \lim_{y \rightarrow +\infty} \int_0^y tf(t)dt$. Considérons la deuxième intégrale. On calcule : $\int_0^y tf(t)dt = \left[-\frac{1}{\sqrt{2\pi}} e^{-t^2/2} \right]_0^y = \frac{1}{\sqrt{2\pi}} (-e^{-y^2/2} + 1)$, qui a pour limite $\frac{1}{\sqrt{2\pi}}$ lorsque y tend vers $+\infty$. De la même manière, la première intégrale tend vers $-\frac{1}{\sqrt{2\pi}}$ lorsque x tend vers $-\infty$. Il en résulte que la somme de ces deux limites vaut 0, i.e. $E(X) = 0$.

- Calculons, sans se focaliser cette fois-ci sur l'intégrale impropre : $V(X) = \int_{-\infty}^{+\infty} t^2 f(t) dt = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} t^2 e^{-t^2/2} dt = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} t \cdot t e^{-t^2/2} dt$ que l'on intègre par parties :

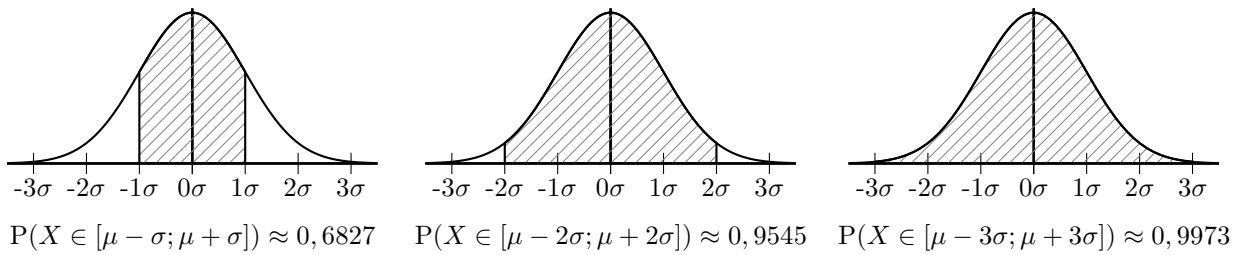
$$\frac{1}{\sqrt{2\pi}} \left[-t e^{-t^2/2} \right]_{-\infty}^{+\infty} - \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} -e^{-t^2/2} dt = 0 + \int_{-\infty}^{+\infty} \frac{1}{\sqrt{2\pi}} e^{-t^2/2} dt = 1.$$

□

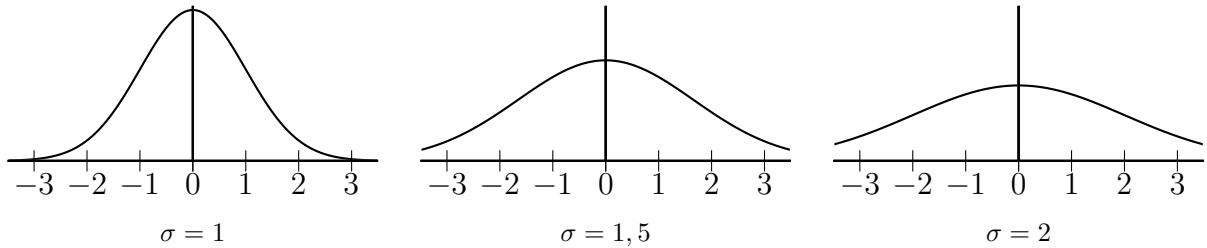
13.5.2 Loi générale

Définition. Soit X une v.a. Si $\frac{X - \mu}{\sigma}$ suit la loi $\mathcal{N}(0; 1)$ alors X suit la *loi normale* $\mathcal{N}(\mu, \sigma^2)$.

Remarque. Si $X \sim \mathcal{N}(\mu, \sigma^2)$ alors on calcule avec un logiciel :



Remarque. La valeur de σ influence l'étalement de la densité :



Théorème. Soit X une v.a. suivant la loi $\mathcal{N}(\mu, \sigma^2)$. Alors :

- $E(X) = \mu$;
- $V(X) = \sigma^2$.

Preuve. On note $Z = \frac{X - \mu}{\sigma}$; on a ainsi $Z \sim \mathcal{N}(0, 1)$ (par définition) et $X = \sigma Z + \mu$.

- $E(X) = E(\sigma Z + \mu) = \sigma E(Z) + E(\mu) = \sigma \cdot 0 + \mu = \mu$.
- $V(X) = V(\sigma Z + \mu) = V(\sigma Z) = \sigma^2 \cdot V(Z) = \sigma^2 \cdot 1 = \sigma^2$.

□

13.6 Fluctuation et estimation

13.6.1 Intervalle de fluctuation

Définition. Un *intervalle de fluctuation asymptotique* d'une v.a. Y_n au seuil $1 - \alpha$ est un intervalle I_n qui contient Y_n avec une probabilité égale à $1 - \alpha$ lorsque n tend vers l'infini, i.e.

$$\lim_{n \rightarrow +\infty} P(Y_n \in I_n) = 1 - \alpha.$$

Théorème. Si X_n suit la loi $\mathcal{B}(n, p)$ alors pour tout $\alpha \in]0; 1[$ on a $\lim_{n \rightarrow +\infty} P\left(\frac{X_n}{n} \in I_n\right) = 1 - \alpha$

$$\text{où } I_n = \left[p - u_\alpha \frac{\sqrt{p(1-p)}}{\sqrt{n}}; p + u_\alpha \frac{\sqrt{p(1-p)}}{\sqrt{n}} \right].$$

Preuve. Soit $X_n \sim \mathcal{B}(n, p)$. Le théorème de Moivre-Laplace et la définition de u_α montrent que

$$\lim_{n \rightarrow +\infty} P\left(-u_\alpha \leq \frac{X_n - np}{\sqrt{np(1-p)}} \leq u_\alpha\right) = P(-u_\alpha \leq X \leq u_\alpha) = 1 - \alpha, \text{ où } X \sim \mathcal{N}(0, 1). \text{ On re-}$$

$$\text{marque ensuite que } -u_\alpha \leq \frac{X_n - np}{\sqrt{np(1-p)}} \leq u_\alpha \Leftrightarrow -u_\alpha \sqrt{np(1-p)} \leq X_n - np \leq u_\alpha \sqrt{np(1-p)} \Leftrightarrow$$

$$np - u_\alpha \sqrt{np(1-p)} \leq X_n \leq np + u_\alpha \sqrt{np(1-p)} \Leftrightarrow p - u_\alpha \frac{\sqrt{p(1-p)}}{\sqrt{n}} \leq \frac{X_n}{n} \leq p + u_\alpha \frac{\sqrt{p(1-p)}}{\sqrt{n}}. \quad \square$$

Remarque. $\frac{X_n}{n}$ représente la fréquence du nombre de succès de la binomiale X_n .

Corollaire. L'intervalle de fluctuation de $\frac{X_n}{n}$ au seuil de 95% est alors à peu près :

$$\left[p - 1,96 \frac{\sqrt{p(1-p)}}{\sqrt{n}}; p + 1,96 \frac{\sqrt{p(1-p)}}{\sqrt{n}} \right].$$

Preuve. Il s'agit juste de se souvenir que $u_{0,05} \approx 1,96$. \square

Remarque. • Il est courant de considérer l'approximation asymptotique comme acceptable lorsque $n \geq 30$, $np \geq 5$ et $np(1-p) \geq 5$. Il ne faut cependant pas considérer cet usage comme une règle absolue mais plutôt comme un ordre d'idée.

- On a déjà vu que $p(1-p) \leq 0,25$ et par conséquent $1,96 \frac{\sqrt{p(1-p)}}{\sqrt{n}} \leq \frac{1}{\sqrt{n}}$, valeur qui a été utilisée en seconde.

13.6.2 Estimation

Définition. Un *intervalle de confiance* pour une proportion p à un niveau de confiance $1 - \alpha$ est un intervalle aléatoire contenant la proportion p avec une probabilité supérieure à $1 - \alpha$, réalisé à partir d'un échantillon.

Théorème. Soient p une proportion fixée et $X_n \sim \mathcal{B}(n, p)$.

Lorsque n tend vers l'infini, l'intervalle :

$$\left[\frac{X_n}{n} - u_\alpha \frac{\sqrt{p(1-p)}}{\sqrt{n}}; \frac{X_n}{n} + u_\alpha \frac{\sqrt{p(1-p)}}{\sqrt{n}} \right]$$

contient la proportion p avec une probabilité de $1 - \alpha$.

Preuve. Il s'agit d'une simple réécriture du théorème de fluctuation asymptotique. En effet on peut écrire $\frac{X_n}{n} \leq p + u_\alpha \frac{\sqrt{p(1-p)}}{\sqrt{n}} \Leftrightarrow \frac{X_n}{n} - u_\alpha \frac{\sqrt{p(1-p)}}{\sqrt{n}} \leq p$ et de la même manière $p - u_\alpha \frac{\sqrt{p(1-p)}}{\sqrt{n}} \leq \frac{X_n}{n} \Leftrightarrow p \leq \frac{X_n}{n} + u_\alpha \frac{\sqrt{p(1-p)}}{\sqrt{n}}$. \square

Corollaire. Soit p une proportion fixée. Lorsque n est assez grand, l'intervalle :

$$\left[\frac{X_n}{n} - \frac{1}{\sqrt{n}}; \frac{X_n}{n} + \frac{1}{\sqrt{n}} \right]$$

contient la proportion p avec une probabilité d'au moins 0,95.

Preuve. C'est encore une reprise de la section précédente, où l'on a vu que $u_{0,05}\sqrt{p(1-p)} < 1$. La limite $1 - \alpha$ du théorème précédent est donc $> 0,95$ et il existe donc un rang n_0 à partir duquel la probabilité que p soit dans l'intervalle ci-dessus est $> 0,95$. \square

Remarque. • La proportion p est alors un élément de l'intervalle $\left[\frac{X_n}{n} - \frac{1}{\sqrt{n}}; \frac{X_n}{n} + \frac{1}{\sqrt{n}} \right]$ avec un *niveau de confiance* de plus de 95%.

- On considèrera ici encore, de manière indicative, que l'approximation est acceptable lorsque $n \geq 30$, $np \geq 5$ et $np(1-p) \geq 5$.
- L'intervalle de confiance ne nécessite pas ici de connaître la proportion p a priori.

13.7 Exercices

Coefficients binomiaux

13.1. Simplifier les expressions suivantes :

1. $\frac{n!}{(n-4)!}$;
2. $\frac{(n+2)!}{(n-1)!}$;
3. $\frac{1}{n!} - \frac{1}{(n+1)!}$.

13.2. Calculer $\binom{666}{3}$ sans utiliser la fonction idoine de la calculatrice.

13.3. Redémontrer la propriété de symétrie et la relation de Pascal par des calculs directs.

- 13.4.**
1. Développer $(x+y)^5$.
 2. Développer $(x-y)^6$.

13.5. Conjecturer puis calculer les sommes suivantes, en appliquant la formule du binôme :

1. $\sum_{k=0}^n \binom{n}{k}$;
2. $\sum_{k=0}^n (-1)^k \binom{n}{k}$.

Schéma de Bernoulli et loi binomiale

13.6. Quelle est la variance maximale d'une loi de Bernoulli ? Pouvait-on prévoir ce résultat ?

13.7. Si $X \sim \mathcal{B}(n, p)$ et $Y \sim \mathcal{B}(n', p)$ sont indépendantes, quelle est alors la loi de $X + Y$?

13.8. Le professeur principal d'une terminale S estime que sa classe de 30 élèves mérite 90% de réussite au bac. Quelle est la probabilité que le taux de réussite soit supérieur à 95% ?

13.9. La moitié de la population française préfère le bleu ; l'autre moitié, le rose. On effectue un sondage sur 1000 personnes pour connaître leur couleur préférée. Quelle est la probabilité qu'au moins 52% des sondés préfèrent le bleu ?

Densité

13.10. La densité de probabilité de présence radiale de l'électron d'un atome d'hydrogène à l'état fondamental est donnée par $d(r) = 4a_0^{-3}r^2e^{-2r/a_0}$ où $a_0 \approx 5,291772 \cdot 10^{-11}\text{m}$ est le *rayon de Bohr*.

1. Montrer que d est bien une densité de probabilité.
2. Calculer la distance moyenne d'un électron au centre de l'atome.

Loi uniforme

13.11. Soient $X \sim \mathcal{U}([a; b])$ et $U \sim \mathcal{U}([0; 1])$.

1. Calculer ex-nihilo la variance de U .
2. Exprimer X en fonction de U .
3. Retrouver la variance de X .

13.12. J'ai, comme souvent, rendez-vous avec Scarlett entre 20h et 20h30 pour un dîner. Malheureusement, elle oublie de venir une fois sur deux. Il est 20h20 ; quelle est la probabilité qu'elle m'ait posé un lapin ?

13.13. On sort : n amis ont rendez-vous au restaurant entre 20h et 20h30. Tous arrivent aléatoirement et indépendamment dans cette plage horaire. On note M l'heure du dernier arrivé.

1. Déterminer la loi de M , en s'intéressant à sa fonction de répartition.
2. Quelle est l'heure moyenne d'arrivée du dernier ?
3. Quelle est la probabilité que le dernier arrive avant 20h20 ? son heure moyenne d'arrivée ? Quelle est la limite de cette heure lorsque n tend vers $+\infty$?

13.14. Soient X et Y deux variables aléatoires indépendantes de loi uniforme sur $[0; 1]$. Soit $Z = X + Y$.

1. Quelles sont les valeurs prises par Z ?
2. Soit $z \in [0; 2]$. Dessiner $A_z = \{(x, y) \in [0; 1]^2, 0 \leq x + y \leq z\}$.
3. Calculer $P((X, Y) \in A_z)$.
4. Déterminer la fonction de répartition de Z puis sa densité.

13.15. Soient X et Y deux variables aléatoires indépendantes de loi uniforme sur $[0; 1]$. Soit $Z = |X - Y|$ (l'écart entre X et Y).

1. En s'inspirant de l'exercice précédent, déterminer la loi de Z .
2. *Application.* Deux personnes ont rendez-vous entre 20h et 21h. Chacune arrive au hasard dans ce laps de temps et attend un quart d'heure avant de partir dégue. Calculer la probabilité que les deux personnes se rencontrent.

Loi exponentielle

13.16 (loi sans mémoire). On se donne une durée de vie aléatoire T d'un individu supposé sans vieillissement (peut-être un extra-terrestre vivant sur une planète très froide ?), i.e. la probabilité que l'individu soit vivant à l'instant $t + h$ sachant qu'il est vivant à l'instant t ne dépend pas de t , où $t \geq 0$ et $h \geq 0$.

1. (a) Que signifie l'évènement $\{T \geq t\}$? Que vaut $\{T \geq 0\}$?
(b) Traduire l'absence de vieillissement en termes de probabilités conditionnelles.

- (c) Montrer que $P_{T \geq t}(T \geq t + h) = P(T \geq h)$.
- (d) En déduire que $\frac{P(T \geq t + h)}{P(T \geq t)} = P(T \geq h)$.
- 2. On définit $\varphi(t) = P(T \geq t)$, que l'on suppose dérivable.
 - (a) Pourquoi est-il raisonnable de supposer que φ est non nulle ?
 - (b) Vérifier que $\varphi(t + h) = \varphi(t)\varphi(h)$.
 - (c) Montrer qu'il existe un réel α tel que $\varphi(t) = e^{\alpha t}$, puis justifier que $\alpha < 0$.
 - (d) Montrer que $P(T < t) = 1 - e^{-\lambda t}$ où $\lambda = -\alpha$.
 - (e) En déduire la densité de T .
- 3. Réciproquement, montrer qu'une variable aléatoire T à densité $\lambda e^{-\lambda t}$ est sans vieillissement.

13.17. La durée de vie (en heures) d'une vitre du rez-de-chaussée du lycée René Perrin est modélisée par une variable aléatoire X suivant une loi exponentielle de paramètre $\lambda = 0,00026$.

1. Calculer $P(X \leq 1000)$ et $P(X > 1000)$.
2. Sachant que $X > 1000$, calculer la probabilité que $X > 2000$.
3. Sachant que la vitre n'a pas été cassée pendant sa vie de 2000 heures, quelle est la probabilité qu'elle soit cassée avant ses 3000 heures ?

13.18. Le laboratoire de physique appliquée du lycée dispose d'un parc d'oscilloscopes identiques. Leur durée de vie (en années) est modélisée par une variable aléatoire X sans vieillissement de paramètre λ .

1. Sachant que $P(X > 10) = 0,286$, montrer que $\lambda \approx 0,125$. On prendra $\lambda = 0,125$ dans la suite.
2. Calculer la probabilité qu'un oscilloscope ait une durée de vie inférieure à 6 mois.
3. Sachant qu'un appareil a déjà fonctionné durant 8 ans, quelle est la probabilité qu'il ait une durée de vie supérieure à 10 ans ?
4. On suppose que les oscilloscopes sont indépendants. Le responsable du laboratoire décide de commander 15 oscilloscopes. Calculer la probabilité qu'au moins un oscilloscope ait une durée de vie supérieure à 10 ans.
5. Combien d'oscilloscopes devrait acheter le responsable afin que la probabilité qu'au moins l'un d'entre eux fonctionne plus de 10 ans soit supérieure à 0,999 ?

13.19. Une entreprise d'autocars dessert le Beaufortain. En chemin, les véhicules peuvent être bloqués par des éléments extérieurs comme la neige, les chutes de pierres, les vaches... Un autocar part du dépôt. On note D la variable aléatoire qui mesure la distance en km qu'il va parcourir sans incident. On considère que sur les kilométrages étudiés le car est sans usure, et on admet que D suit une loi exponentielle de paramètre $\lambda = \frac{1}{82}$.

1. Calculer la probabilité que la distance parcourue sans incident soit :
 - (a) comprise entre 50 et 100 km ;

- (b) supérieure à 300 km.
- 2. Sachant que l'autocar a déjà parcouru 350 km sans incident, quelle est la probabilité qu'il n'en subisse pas non plus au cours des 25 km suivants ?
- 3. L'entreprise possède N autocars indépendants. On note X_d la variable aléatoire égale au nombre d'autocars n'ayant subi aucun incident après avoir parcouru d km.
 - (a) Montrer que X_d suit une loi binomiale $\mathcal{B}(N, e^{-\lambda d})$.
 - (b) Calculer le nombre moyen d'autocars n'ayant subi aucun incident après avoir parcouru d kilomètres.

13.20. Les ampoules basse consommation sont considérées comme ne s'usant pas. Dans une pièce, on installe deux telles ampoules indépendantes, de durées de vie moyennes 5000 et 10000 heures. Quelle est la durée moyenne avant le changement de la première ampoule hors-service ?

Loi normale

13.21. Montrer que la courbe de Gauss possède deux points d'inflexion que l'on précisera.

13.22. Soient $X \sim \mathcal{N}(\mu; \sigma^2)$, F sa fonction de répartition et f sa densité.

1. Montrer que $F(x) = \phi\left(\frac{x-\mu}{\sigma}\right)$.
2. En déduire que $f(x) = \frac{1}{\sigma\sqrt{2\pi}}e^{-(x-\mu)^2/2\sigma^2}$.

13.23. Soit $X \sim \mathcal{N}(0, 1)$. Calculer :

1. $P(X < 1,47)$;
2. $P(X \leq 3,2)$;
3. $P(X < -1,47)$;
4. $P(X > 0,94)$;
5. $P(X \geq -2,32)$;
6. $P(1,13 < X < 2,86)$;
7. $P(-1,72 \leq X \leq -0,62)$;
8. $P(-1,2 < X < 0,23)$.

13.24. Soit $X \sim \mathcal{N}(2; 0,3^2)$. Calculer directement puis en se ramenant à une loi centrée réduite :

1. $P(X < 1,47)$;
2. $P(X \leq 3,2)$;
3. $P(X < -1,47)$;
4. $P(X > 0,94)$;
5. $P(X \geq -2,32)$;
6. $P(1,13 < X < 2,86)$.

13.25. Soit $X \sim \mathcal{N}(2, 5; 0, 2^2)$. Déterminer α tel que $P(X < \alpha) = 0,67$.

13.26. Soit $X \sim \mathcal{N}(2, 5; 0, 2^2)$. Donner $E(X)$, $\sigma(X)$ et $V(X)$.

13.27. Une machine fabrique des résistors. La variable aléatoire X associée à chaque résistor sa résistance exprimée en ohms. On suppose que X suit une loi normale de moyenne $m = 100$ et d'écart-type $\sigma = 3$.

1. On prélève un résistor au hasard dans la production. Il est considéré comme conforme si sa résistance est comprise entre 94,75 et 105,25 ohms. Calculer la probabilité qu'un résistor ne soit pas conforme.
2. Déterminer le réel a tel que 97% des résistors produits par la machine aient une résistance comprise entre $100 - a$ et $100 + a$.

13.28. Une machine fabrique des condensateurs de $5 \mu F$ en très grande série. La capacité X de ces condensateurs suit une loi normale de moyenne $\bar{X} = 4,96 \mu F$ et d'écart-type $\sigma = 0,05 \mu F$. On considère qu'un condensateur est acceptable si sa capacité est comprise entre $4,85 \mu F$ et $5,15 \mu F$. La machine est considérée comme bien réglée si 99% de sa production est acceptable.

1. Calculer la probabilité qu'un condensateur soit acceptable.
La machine est-elle bien réglée?
2. On prélève un échantillon de 10 condensateurs de la production.
Quelle est la probabilité qu'au moins 9 d'entre eux soient acceptables?
3. On souhaite accélérer la production, quitte à diminuer la qualité; l'écart-type σ va donc augmenter. On en profite pour régler correctement la machine sur $\bar{X} = 5 \mu F$. Déterminer σ afin que 80% de la production soit acceptable.

13.29. Une machine fabrique un très grand nombre de pièces d'un même modèle. Une pièce fabriquée est conforme si son épaisseur est comprise en 14,3 et 15,5 mm.

On considère la variable aléatoire X qui, à chaque pièce prélevée au hasard dans la production d'une journée, associe son épaisseur en millimètres. La variable aléatoire X suit la loi normale de moyenne m et d'écart type σ . La moyenne m dépend du réglage de la machine.

1. Dans cette question, on suppose que $\sigma = 0,35$ et $m = 15$.
 - (a) Calculer la probabilité qu'une pièce prélevée soit conforme.
 - (b) Calculer le nombre réel positif h tel que $P(15 - h \leq X \leq 15 + h) = 0,95$.
2. La machine est désormais réglée de sorte que $m = 14,9$.
Quel devrait être alors l'écart type pour que le pourcentage de pièces conformes soit égal à 90%?

13.30. Les joueurs d'échecs sont évalués suivant le *classement Elo*. Pour donner un ordre d'idée, les joueurs sont classés entre 1000 et 2900. Le principe est le suivant : si les joueurs A et B ont des classements α et β alors la probabilité que A batte B est $F(\alpha - \beta)$ où F est la fonction de répartition de la loi $\mathcal{N}(0, (200\sqrt{2})^2)$.

1. Quelle est la probabilité que le meilleur joueur du monde, classé 2870, batte le meilleur Français, classé 2730?

2. Un joueur classé 1850 a fait un grand nombre de parties contre un de ses amis. Il en a gagné seulement 30%; quel est le classement supposé de son ami joueur?

13.31. Un groupe de 10 coureurs se donne rendez-vous pour gravir le Mont Charvin. On estime que les coureurs de ce groupe mettent en moyenne 1 heure avec un écart-type de 5 minutes. De multiples paramètres indépendants et aux conséquences minimes influent sur la durée T de l'ascension; on peut ainsi raisonnablement supposer qu'elle suit une loi normale.

1. Donner les paramètres de la loi normale de T .
2. Le groupe décide une course amicale pour grimper au sommet, en partant à 11 heures. Ils décident qu'ils mangeront tous ensemble au sommet.
Quelle est la probabilité qu'ils commencent à déjeuner après 12h10?

Approximation normale de la loi binomiale, fluctuation et estimation

13.32. On effectue un sondage sur 1000 personnes concernant leurs intentions de vote au second tour d'une élection présidentielle. Deux candidats sont en lice : Alfred et Mario.

1. Dans cette question, on analyse a posteriori le sondage et on suppose donc connu le résultat de l'élection : $p = 52\%$ des électeurs ont voté pour Alfred.
 - (a) Quelle est la loi du nombre de sondés ayant déclaré vouloir voter pour Alfred?
 - (b) Par quelle loi peut-on l'approcher raisonnablement?
 - (c) Quelle est la probabilité que le sondage donne Mario vainqueur?
 - (d) Quel intervalle de fluctuation asymptotique au seuil de 95% peut-on donner pour le résultat du sondage?
 - (e) Combien de personnes aurait-il fallu interroger afin que le résultat du sondage donne le bon vainqueur avec une probabilité de 95%? de 99%?
2. On suppose maintenant qu'on ne connaît pas le résultat p de l'élection, ce qui est tout de même plus courant pour un sondage.
 - (a) Déterminer un intervalle pour p au niveau de confiance de plus de 95%.
 - (b) Déterminer un intervalle pour p au niveau de confiance de plus de 99%.
 - (c) Combien faudrait-il interroger de personnes afin qu'on puisse donner p à 1% près avec un niveau de confiance de 95%?

13.33. On souhaite estimer la superficie du lac d'Annecy. Sur une image satellitaire de taille 20 km sur 15 km contenant le lac, les élèves de spécialité ISN ont tiré au hasard 500 points. Par une analyse des couleurs, ils ont déterminé que 49 d'entre eux sont sur le lac.

1. Déterminer une approximation de la superficie du lac.
2. Quel intervalle de confiance au niveau de 95% peut-on donner pour sa superficie réelle?
3. Quel encadrement de la superficie du lac peut-on donner au niveau de confiance de 99%?
4. Combien de points faudrait-il tirer au hasard afin d'obtenir un encadrement à $\pm 1\text{km}^2$ au niveau de confiance de 95%?

13.34. On reprend l'étude de la méthode de Monte-Carlo, destinée à calculer une approximation numérique d'une intégrale.

Soit f une fonction continue et positive sur un intervalle $[a; b]$, majorée par M . On tire un point au hasard dans le rectangle $[a; b] \times M$; si ce point est sous la courbe on compte 1, sinon on compte 0. On répète cette expérience n fois et on note S_n le résultat obtenu.

1. Quelle approximation de $I = \int_a^b f$ peut-on donner ?
2. Quelle est la loi de S_n ?
3. On s'intéresse ici à $I = \int_0^1 x^2 dx$. On rappelle que $I = \frac{1}{3}$.
 - (a) Quel intervalle de fluctuation peut-on donner pour I au seuil de $1 - \alpha$? de 95% ? de 99% ?
 - (b) Déterminer ces intervalles lorsque $n = 1000$.
 - (c) Combien de points faudrait-il tirer afin qu'on puisse approcher I à 10^{-3} près au seuil de 95% ? La méthode de Monte-Carlo est-elle ici efficace ?
4. Considérons maintenant le cas général, où la valeur de l'intégrale I est inconnue.
 - (a) Quel intervalle de confiance simplifié au seuil de 95% peut-on donner pour I ?
 - (b) Comment a-t-on ici intérêt à choisir le majorant M ?
 - (c) Si l'on utilise l'intervalle de confiance (non simplifié) avec $u_{0,05}$, la valeur du majorant M influe-t-elle sur l'encadrement proposé ?

Partie II

Cours et exercices – Spécialité

1. Divisibilité

1.1 Divisibilité dans \mathbb{Z}

1.1.1 Multiples et diviseurs

Définition. Un nombre *entier* est par défaut un entier relatif (de \mathbb{Z}). Si ce nombre est positif alors c'est un entier *naturel* (de \mathbb{N}).

Définition. Soient a et b dans \mathbb{Z} . Le nombre a est un *multiple* de b (ou b est un *diviseur* de a) s'il existe k dans \mathbb{Z} vérifiant $a = kb$.

Remarque. • On note alors $b|a$.

- L'ensemble des multiples de a est noté $a\mathbb{Z}$. Par exemple les nombres pairs sont notés $2\mathbb{Z} = \{\dots, -4, -2, 0, 2, 4, 6, \dots\}$.
- Tout entier a possède au moins comme diviseurs $1, -1, a, -a$.
- Si $a \neq 0$ alors tout diviseur de a est compris entre $-|a|$ et $|a|$. Il en résulte qu'un entier non nul possède un *nombre fini* de diviseurs.

1.1.2 Propriétés élémentaires

On se place dans \mathbb{Z} .

1. Si $b|a$ alors $-b|a$ aussi.
2. Si $a|b$ et $b|a$ alors $a = \pm b$.
3. Si $a|b$ et $b|c$ alors $a|c$ (transitivité).
4. Si $a|b$ et $a|c$ alors a divise $b + c$, $b - c$ et plus généralement toute combinaison linéaire $\lambda b + \mu c$.
5. Si $a|b$ alors $ac|bc$ pour tout c non nul.

Preuve. Exercice!

□

1.2 Division euclidienne

1.2.1 Préliminaires

On rappelle le résultat fondamental (découlant de la construction de \mathbb{N}) suivant :

Théorème. Toute partie non vide de \mathbb{N} possède un plus petit élément.

Remarque. Cette propriété est remarquable. Elle est par exemple fausse pour \mathbb{R}_+ (\mathbb{R}_+^* ne possède pas de plus petit élément) et \mathbb{Q}_+ (\mathbb{Q}_+^* ne possède pas de plus petit élément).

Théorème. Toute suite décroissante d'entiers naturels est stationnaire.

Preuve. Soit (a_n) une suite décroissante d'entiers naturels et soit $A = \{a_n, n \in \mathbb{N}\}$ l'ensemble des valeurs prises par cette suite. L'ensemble A d'entiers naturels possède un plus petit élément a_∞ . Il existe donc un rang n_0 tel que $a_{n_0} = a_\infty$. Puisque (a_n) décroît, $n \geq n_0$ implique $a_n = a_{n_0}$. \square

1.2.2 Division euclidienne

Théorème. Soient a et b deux entiers naturels, avec $b \neq 0$. Il existe un unique couple (q, r) d'entiers naturels vérifiant $a = bq + r$ et $0 \leq r < b$.

Définition. Dans cette situation, a est le *dividende*, b le *diviseur*, q le *quotient* et r le *reste*.

Preuve.

- *Existence.* Soit $B = \{k \in \mathbb{N}, kb > a\}$ l'ensemble de tous les multiples de b supérieurs à a . C'est un sous-ensemble de \mathbb{N} , il possède ainsi un plus petit élément q' . Notons alors $q = q' - 1$. Par définition de q' , $qb \leq a$. Ainsi $r = a - bq \geq 0$ et de plus $r < b$ (sinon $r \geq b$ implique $a - bq \geq b$ i.e. $a \geq b + bq = q'b$: absurde).
- *Unicité.* Si $a = bq_1 + r_1 = bq_2 + r_2$ avec $0 \leq r_1, r_2 < b$ alors $-b < r_2 - r_1 < b$ et $r_2 - r_1 = b(q_1 - q_2)$. Ainsi $r_2 - r_1$ est un multiple de b strictement compris entre $-b$ et b ; la seule possibilité est $r_2 - r_1 = 0$. Par conséquent $r_1 = r_2$ et ensuite $q_1 = q_2$. \square

Corollaire. Soient a et b deux entiers relatifs, avec $b \neq 0$. Il existe un unique couple (q, r) avec $q \in \mathbb{Z}$ et $r \in \mathbb{N}$ vérifiant $a = bq + r$ et $0 \leq r < |b|$.

1.3 Pgcd, ppcm, algorithme d'Euclide

1.3.1 Pgcd, ppcm

Théorème. Soient a et b deux entiers non nuls.

- L'ensemble des diviseurs communs à a et b possède un plus grand élément noté $a \wedge b$ ou $\text{pgcd}(a, b)$ (*plus grand commun diviseur*).
- L'ensemble des multiples communs strictement positifs à a et b possède un plus petit élément noté $a \vee b$ ou $\text{ppcm}(a, b)$ (*plus petit commun multiple*).

Preuve.

- L'ensemble des diviseurs communs à a et b contient 1; il est donc non vide et par ailleurs fini. Il possède donc un plus grand élément.
- L'ensemble des multiples communs strictement positifs à a et b contient $|ab|$; il est donc une partie non vide de \mathbb{N} . Il possède donc un plus petit élément (propriété fondamentale de \mathbb{N}). \square

Remarque. Le pgcd divise a et le ppcm est un multiple de a donc le pgcd divise le ppcm.

Définition. Deux entiers sont *premiers entre eux* si leur pgcd vaut 1.

Remarque. Soient a et b deux entiers non nuls et d leur pgcd. On a donc $a = da'$ et $b = db'$ avec a' et b' entiers. Soit d' leur pgcd ; il divise a' et b' et donc dd' divise a et b . L'option $d' > 1$ conduit donc à une absurdité puisque d est le plus grand diviseur commun de a et b . Finalement $d' = 1$ i.e. a' et b' sont premiers entre eux.

1.3.2 Calcul effectif du pgcd

Théorème (Euclide). Soient a et b deux entiers naturels non nuls et $a = bq + r$ leur division euclidienne. Alors $\text{pgcd}(a, b) = \text{pgcd}(b, r)$

Preuve. Si c divise a et b alors c divise $a - bq = r$. Réciproquement, si c divise b et r alors c divise $bq + r = a$. Ainsi l'ensemble des diviseurs communs à a et b et celui des diviseurs communs à b et r sont les mêmes. Ils possèdent donc le même plus grand élément. \square

Théorème (algorithme d'Euclide). L'itération de l'égalité du théorème précédent permet de trouver le pgcd de a et b comme le dernier reste r non nul.

Preuve. On a successivement $\text{pgcd}(a, b) = \text{pgcd}(b, r_0)$, $\text{pgcd}(b, r_0) = \text{pgcd}(r_0, r_1)$, $\text{pgcd}(r_0, r_1) = \text{pgcd}(r_1, r_2)$, $\text{pgcd}(r_1, r_2) = \text{pgcd}(r_2, r_3)$, etc. La suite (r_k) des restes est strictement décroissante (car un reste est strictement inférieur au diviseur) ; elle s'arrête donc et on note r_{n-1} le dernier reste non nul.

Par égalités successives, $\text{pgcd}(a, b) = \dots = \text{pgcd}(r_{n-2}, r_{n-1})$. De plus $r_{n-2} = qr_{n-1} + r_n = qr_{n-1}$ implique $\text{pgcd}(r_{n-2}, r_{n-1}) = r_{n-1}$. Finalement, $\text{pgcd}(a, b) = r_{n-1}$. \square

Remarque. On peut attaquer l'algorithme d'Euclide sans tenir compte du plus grand des deux entiers a et b . Un mauvais choix éventuel (i.e. par un programme) se traduit par une simple division euclidienne inutile.

1.4 Congruences

1.4.1 Généralités

Définition. Deux entiers a et b sont *congrus* modulo l'entier naturel n si $a - b$ est un multiple de n . On note alors $a \equiv b \pmod{n}$ ou $a \equiv b [n]$.

Remarque. De manière équivalente, ceci signifie que a et b ont le même reste lors de leur division euclidienne par n .

Remarque. Il existe un seul entier r vérifiant $0 \leq r < n$ et $a \equiv r \pmod{n}$. C'est le *résidu minimal*. La phrase « calculer $a \pmod{n}$ » signifie « calculer r » (*réduction modulaire*).

Théorème.

- (réflexivité) $a \equiv a \pmod{n}$;
- (commutativité) $a \equiv b \pmod{n}$ ssi $b \equiv a \pmod{n}$;
- (transitivité) $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$ impliquent $a \equiv c \pmod{n}$.

Preuve. Triviale. \square

1.4.2 Opérations

Théorème. • Si $a \equiv b \pmod n$ et $a' \equiv b' \pmod n$ alors $a + a' \equiv b + b' \pmod n$;

- si $a \equiv b \pmod n$ et $a' \equiv b' \pmod n$ alors $aa' \equiv bb' \pmod n$;
- si $a \equiv b \pmod n$ et $k \in \mathbb{N}$ alors $a^k \equiv b^k \pmod n$.

Preuve. • Exercice !

- Il suffit de remarquer que $aa' - bb' = (a - b)a' + (a' - b')b$ est divisible par n puisque $a - b$ et $a' - b'$ le sont.
- Simple récurrence en utilisant le deuxième point : exercice !

□

Remarque. Attention ! il n'y a pas d'opération triviale de division modulaire.

1.5 Grands théorèmes

1.5.1 Bézout

Théorème (de Bézout). Deux entiers non nuls a et b sont premiers entre eux ssi il existe deux entiers u et v vérifiant $au + bv = 1$.

Preuve. • Supposons qu'il existe u et v tels que $au + bv = 1$. Si d divise a et b alors d divise $au + bv$ i.e. $d = 1$. Par conséquent a et b sont premiers entre eux.

- Supposons que a et b soient premiers entre eux. Posons $G = \{am + bn, m \in \mathbb{Z}, n \in \mathbb{Z}\} \cap \mathbb{N}^*$. On constate que G est non vide puisque $aa + bb = a^2 + b^2 > 0$ et donc $aa + bb \in G$. L'ensemble G est donc un sous-ensemble non vide de \mathbb{N}^* et possède ainsi un plus petit élément non nul $d = au + bv$. Montrons ensuite que d divise a et b . Effectuons la division euclidienne de a par d : $a = dq + r$ avec $0 \leq r < d$. Il vient $r = a - dq = a - (au + bv)q = a(1 - qu) + b(-vq)$. Si $r > 0$ alors on a trouvé un élément de G plus petit que d car $r < d$, ce qui contredit la définition de d . Ainsi $r = 0$, ce qui montre que d divise a . En montrant de même que d divise b , on prouve que d divise a et b . Puisque a et b sont premiers entre eux, on obtient $d = 1$ et finalement $au + bv = 1$.

□

Corollaire. L'équation diophantienne $ax + by = c$ ($a, b \in \mathbb{Z}^*$, $c, x, y \in \mathbb{Z}$) possède des solutions ssi c est un multiple de $d = \text{pgcd}(a, b)$.

Preuve. • Supposons qu'il existe x et y tels que $ax + by = c$. Il suffit de noter que d divise a et b donc $ax + by$ i.e. d divise c .

- Posons, comme nous l'avons déjà vu, $a = da'$ et $b = db'$ avec a' et b' premiers entre eux. Le théorème de Bézout montre qu'il existe deux entiers u et v vérifiant $a'u + b'v = 1$. Ainsi $da'u + db'v = d$, soit $au + bv = d$. Si c est un multiple de d ($c = kd$) alors $a(ku) + b(kv) = kd = c$.

□

Corollaire. Un diviseur commun à deux entiers divise leur pgcd.

Preuve. Soient a et b deux entiers non nuls et d leur pgcd. On sait désormais qu'il existe deux entiers u et v tels que $au + bv = d$. Si d' divise a et b alors d' divise $au + bv$ i.e. d' divise d . \square

Corollaire (inverse modulaire). Un entier non nul a possède un *inverse* modulo l'entier naturel non nul n (i.e. un entier b tel que $ab \equiv 1 \pmod{n}$) ssi a et n sont premiers entre eux.

Preuve. Par le théorème de Bézout : a et n sont premiers entre eux ssi il existe des entiers u et v vérifiant $au + nv = 1$ ssi $au \equiv 1 \pmod{n}$. \square

Remarque.

- Les solutions d'une équation diophantienne $ax + by = c$ (avec c multiple de $\text{pgcd}(a, b)$) se représentent comme des points régulièrement répartis sur la droite d'équation $ax + by = c$ soit $y = \frac{1}{b}(c - ax)$.
- Ceci conduit à un algorithme simple (mais peu performant) pour trouver une solution particulière de cette équation : on vérifie si $x = 1, 2, 3, \dots$ conduit à un y entier. Dès que c'est le cas, on a trouvé un couple (x, y) solution.

1.5.2 Gauss

Théorème (de Gauss). Soient a, b, c trois entiers non nuls. Si a divise bc et si a est premier avec b alors a divise c .

Preuve. On a $bc = ka$. Puisque a et b sont premiers entre eux, le théorème de Bézout montre qu'il existe deux entiers u et v vérifiant $au + bv = 1$. Il vient $c = c \cdot 1 = c(au + bv) = cau + (cb)v = cau + kav = a(cu + kv)$ i.e. c est un multiple de a . \square

Corollaire. Si a et b divisent c et si a et b sont premiers entre eux alors ab divise c .

Preuve. On remarque que b divise $c = ka$. Puisque b est premier avec a , le théorème de Gauss montre que b divise k ($k = lb$). Il vient $c = ka = lba = l(ab)$ et ainsi ab divise c . \square

1.6 Exercices

Généralités

- 1.1.** 1. Montrer, en effectuant une division euclidienne posée, que le développement décimal d'un rationnel est périodique.
2. Réciproquement, montrer qu'un réel dont le développement décimal est périodique est un rationnel.
3. *Application.*
- (a) Quelle est la période du développement décimal de $\frac{3}{7}$?
- (b) Quelle fraction possède pour développement décimal $0,\overline{63}$?
- 1.2.** Déterminer un entier qui soit un multiple commun de 12 et -15.
- 1.3.** Soit n un entier impair. Montrer que $n^2 - 1$ est divisible par 8.
- 1.4.** Montrer que, quels que soient les entiers a et b , $(a - b)^3 - (a^3 - b^3)$ est divisible par 3.
- 1.5.** Montrer que tout nombre obtenu en répétant une série de 4 chiffres (par exemple 12341234) est divisible par 73.
- 1.6.** Que peut-on dire d'une suite d'entiers naturels strictement décroissante ?

Division euclidienne

- 1.7.** Effectuer la division euclidienne de 3217 par 19, de -1273 par 17, de 228 par -15 et de -329 par -30.
- 1.8.** Déterminer des entiers naturels a et b tels que leur somme soit égale à 283 et que dans la division de a par b , le quotient soit 5 et le reste 13.
- 1.9.** 1. Réaliser la division de $n^2 + 2n + 2$ par $n + 3$ pour montrer que $n^2 + 2n + 2 = (n + 3)(n - 1) + 5$.
2. Déterminer les entiers naturels n tels que le nombre $\frac{n^2 + 2n + 2}{n + 3}$ soit entier.
- 1.10.** Soit n un entier naturel non nul. Effectuer la division euclidienne de :
1. $2n^2 + n$ par $n + 1$;
 2. $n^2 + 2n + 3$ par $n + 2$;
 3. $3^n - 2$ par 3^{n-1} .

Pgcd, ppcm, algorithme d'Euclide

1.11. Calculer les pgcd des entiers suivants en utilisant l'algorithme d'Euclide :

1. 4539 et 1958 ;
2. 1234 et 482 ;
3. 5427 et -1590 ;
4. -3640 et -12325 ;
5. -45045 et 50050.

1.12. 1. Déterminer simplement le pgcd de 2012 et 2013.

2. Soit n un entier. Calculer le pgcd de n et $n + 1$.

1.13. Soit n un entier naturel non nul. Calculer les pgcd possibles des entiers suivants en utilisant l'algorithme d'Euclide ou les opérations sur les diviseurs :

1. $3n + 1$ et $7n + 2$;
2. $5n + 5$ et $8n + 6$;
3. $3n + 1$ et $5n$.

1.14. Soient a et b deux entiers naturels premiers entre eux. Soit la suite (type Fibonacci) (u_n) définie par $u_0 = a$, $u_1 = b$ et $u_{n+2} = u_{n+1} + u_n$.

Montrer par récurrence que deux termes consécutifs de cette suite sont premiers entre eux.

1.15. Déterminer les couples $(a; b)$ d'entiers naturels non nuls tels que $ab = 1734$ et $a \wedge b = 17$.

1.16. Déterminer les couples $(a; b)$ d'entiers naturels non nuls tels que $a + b = 1152$ et $a \wedge b = 64$.

Congruences

1.17. Montrer que $32 \equiv -7 \pmod{13}$.

1.18. Montrer les critères de divisibilité suivants :

1. un entier est divisible par 9 ssi la somme de ses chiffres est divisible par 9 ;
2. un entier est divisible par 3 ssi la somme de ses chiffres est divisible par 3 ;
3. un entier est divisible par 5 ssi son dernier chiffre est 0 ou 5 ;
4. un entier est divisible par 4 ssi le nombre formé par ses deux derniers chiffres est divisible par 4 ;
5. un entier est divisible par 11 ssi la somme alternée de ses chiffres est un multiple de 11.

1.19. La *preuve par 9* consiste en une vérification d'un calcul modulo 9. L'égalité $1\,022\,561\,861 = 54\,014 \times 18\,931 + 22\,837$ est-elle juste ?

1.20. 1. Quel peut être le reste de la division euclidienne par 5 d'un carré ?

2. Quel peut être le reste de la division euclidienne par 7 d'un cube ?

3. Quel peut être le reste de la division euclidienne par 4 d'une somme de deux carrés ?
- 1.21.** 1. Déterminer l'ensemble des entiers x vérifiant $x^5 \equiv x \pmod{5}$.
 2. Déterminer l'ensemble des entiers x tels que $x^2 - x + 1$ soit divisible par 7.
- 1.22.** 1. Calculer $32^{48} \pmod{7}$.
 2. Calculer $247^{349} \pmod{7}$.
 3. Montrer que $2^{3n} - 1$ est un multiple de 7.
 4. Montrer que $3^{n+6} - 3^n$ est divisible par 7.
 5. Calculer $5^{3n} - 6^n \pmod{17}$.
 6. Montrer que $3^{n+3} \equiv 4^{4n+2} \pmod{11}$.
 7. Calculer $5^n \pmod{7}$ après avoir observé ces résultats sur machine.

Applications des théorèmes de Bézout et Gauss

- 1.23.** 1. Montrer que $12 \equiv 42 \pmod{10}$ mais que $\frac{12}{6} \not\equiv \frac{42}{6} \pmod{10}$.
 2. Supposons que $a \equiv b \pmod{n}$ et que k divise a et b . Montrer que si k est premier avec n alors $\frac{a}{k} \equiv \frac{b}{k} \pmod{n}$.
- 1.24.** Soit n un entier naturel non nul. En utilisant le théorème de Bézout, montrer que les entiers suivants sont premiers entre eux :
1. $2n + 1$ et $9n + 4$;
 2. $3n - 2$ et $5n - 3$.
- 1.25.** Résoudre (dans $\mathbb{Z} \times \mathbb{Z}$) l'équation diophantienne $35x - 21y = 14$.
- 1.26.** 1. Déterminer une solution particulière de l'équation diophantienne $62x + 43y = 1$.
 2. Déterminer une solution particulière de l'équation diophantienne $54x + 35y = 11$ en abordant d'abord $54x + 35y = 1$.
- 1.27.** Résoudre les équations diophantiennes suivantes :
1. $17x - 33y = 1$;
 2. $91x + 10y = 41$;
 3. $50x + 9y = 1$;
 4. $144x + 625y = 3$.
- 1.28.** On cherche les entiers x vérifiant $x \equiv 3 \pmod{11}$ et $x \equiv 4 \pmod{15}$.
 1. Montrer que ceci est équivalent à résoudre l'équation $11u + 15v = 1$.
 2. Trouver les entiers x recherchés.
- 1.29.** On cherche les entiers x vérifiant $x \equiv x_0 \pmod{p}$ et $x \equiv x_1 \pmod{q}$.
 Quelle condition sur p et q assure l'existence de solutions ?
- 1.30.** La comète de Halley est venue nous rendre visite en 1986 et possède une période de 76 ans. La comète Hale-Bopp est apparue en 1997 et sa période est de 2537 ans. En quelle année pourra-t-on observer leur conjonction ?

Applications pratiques

1.31. Le numéro INSEE (de sécurité sociale) est formé d'un nombre a de 13 chiffres (sexe, année de naissance, mois de naissance, département de naissance, code de commune, numéro de la naissance) et d'une clé k de 2 chiffres. Cette clé est fabriquée par $k = -a \pmod{97}$.

1. Calculer la clé associée au numéro 1 56 11 13 055 376.
2. Montrer que si un seul chiffre de a est erroné alors l'erreur est détectée.
3. Montrer que si deux chiffres consécutifs de a sont intervertis alors l'erreur est détectée.

1.32. Un code barres est un nombre a de 13 chiffres : 12 chiffres de code produit et 1 chiffre de clé. Si a s'écrit $a_1 \cdots a_{13}$ alors cette clé est calculée de sorte que $3 \sum_{i=1}^6 a_{2i} + \sum_{i=0}^6 a_{2i+1} \equiv 0 \pmod{10}$.

1. Calculer la clé du code produit 3 250 390 176 81.
2. Montrer que si un seul des 13 chiffres est erroné alors l'erreur est détectée.
3. Étudier la situation d'une erreur de permutation de deux chiffres.

1.33. Un numéro de carte bleue est un nombre à 16 chiffres $a_{16} \cdots a_1$. Sur ces chiffres, on définit l'application f par $f(x) = 2x$ si $0 \leq 2x \leq 9$ et sinon par $f(x) = x_1 + x_2$ si $2x = 10x_1 + x_2$. On impose au numéro de vérifier $a_1 + f(a_2) + \cdots + a_{15} + f(a_{16}) \equiv 0 \pmod{10}$.

Montrer que si un seul chiffre est erroné, le numéro n'est plus valide.

1.34 (cryptage affine). On numérise les lettres de l'alphabet par $A = 0, \dots, Z = 25$. On code ces lettres grâce à la fonction $f(x) = 17x + 22 \pmod{26}$.

1. Coder le mot ENNUI.
2. Déterminer la fonction f^{-1} de décodage.
3. Décoder OAYRC.

1.35 (chiffrement de Vigenère). On identifie les lettres de l'alphabet par $A = 0, \dots, Z = 25$. On se donne une clé littérale de longueur quelconque ; celle-ci se traduit par une série d'entiers $k_0 k_1 k_2 k_3 \cdots k_{p-1}$ entre 0 et 25. On code un texte quelconque $t_0 t_1 t_2 t_3 \cdots t_n$ en effectuant $c_i = t_i + k_{(i \bmod p)} \pmod{26}$.

1. Coder « JE SUIS CONTENT DE FAIRE UN DM » avec la clé « YOUPI ».
2. En quoi ce système de cryptage est-il plus résistant que le cryptage affine ?
3. Comment peut-on cependant procéder pour essayer de décoder un long texte ?

2. Nombres premiers

2.1 Généralités

Définition. Un entier naturel est *premier* lorsqu'il ne possède que deux diviseurs positifs, à savoir 1 et lui-même.

Remarque. • Ainsi 0 et 1 ne sont pas premiers.

- Le plus petit nombre premier est 2.
- Un entier qui n'est pas premier est *composé*.
- Les diviseurs de n compris entre 2 et $n - 1$ sont ses *diviseurs propres*; 1 et n sont ses *diviseurs triviaux*.

Théorème. Tout entier naturel $n \geq 2$ admet comme plus petit diviseur propre un entier premier p . Si n est composé, on a de plus $2 \leq p \leq \sqrt{n}$.

Preuve. • Si n est premier alors $p = n$ est trivial. Si n est composé, l'ensemble E des diviseurs ≥ 2 de n est une partie non vide de \mathbb{N} . Il possède donc un plus petit élément p . Si p était composé, il serait divisible par un entier q vérifiant $2 \leq q < p$. Cet entier q diviserait alors n , contrevenant ainsi à la définition de p . Finalement p est premier.

- Si $n = pq$ avec $2 \leq p \leq q$ alors $p^2 \leq pq = n$ d'où $p \leq \sqrt{n}$.

□

Théorème (Euclide). L'ensemble des nombres premiers est infini.

Preuve. Supposons que cet ensemble soit fini : $P = \{p_1, \dots, p_n\}$. L'entier $a = p_1 p_2 \cdots p_n + 1$ ne possède aucun diviseur premier. Le théorème précédent montre que c'est impossible. □

2.2 Décomposition

Théorème. Tout entier ≥ 2 se décompose en produit de facteurs premiers, cette décomposition étant unique à l'ordre près.

Preuve. • *Existence.* Soit $P_n =$ « tout entier compris entre 2 et n possède une décomposition en facteurs premiers ». Pour $n = 2$ c'est trivial. Si P_n est vraie : soit $n + 1$ est premier, soit il est composé et donc est le produit de de entiers $\leq n$ qui se décomposent, par hypothèse, en produit de facteurs premiers. Ainsi $n + 1$ se décompose aussi et P_{n+1} est donc vraie. Par récurrence, P_n est vraie pour tout $n \geq 2$.

- *Unicité.* Voir les éléments qui y conduisent dans les exercices.

□

Remarque. Cette démonstration d'existence n'est pas constructive. L'algorithme (exercice!) de décomposition cherche à diviser un entier n autant que possible par 2, par 3, par 5, etc.

Théorème. Si $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ et $b = p_1^{\beta_1} \cdots p_k^{\beta_k}$, où $\alpha_i, \beta_i \geq 0$ alors $\text{pgcd}(a, b) = p_1^{\min(\alpha_1, \beta_1)} \cdots p_k^{\min(\alpha_k, \beta_k)}$ et $\text{ppcm}(a, b) = p_1^{\max(\alpha_1, \beta_1)} \cdots p_k^{\max(\alpha_k, \beta_k)}$.

Preuve. Exercice. □

Corollaire. Si $d = \text{pgcd}(a, b)$ et $m = \text{ppcm}(a, b)$ alors $dm = ab$.

Preuve. Il suffit essentiellement de noter que $\min(x, y) + \max(x, y) = x + y$. □

2.3 Petit théorème de Fermat

Théorème. Si a est un entier et p un nombre premier alors $a^p \equiv a \pmod{p}$. Si de plus p ne divise pas a alors $a^{p-1} \equiv 1 \pmod{p}$.

Preuve. Voir exercice 2.16. □

Remarque. • Le petit théorème de Fermat a été énoncé par Fermat en 1640, prouvé par Leibniz avant 1683 et publié (et généralisé) par Euler en 1736.

- Il ne faut pas confondre ce résultat avec le grand théorème de Fermat, plus facile à énoncer (*il n'existe pas de solutions entières non triviales de $x^n + y^n = z^n$ pour $n \geq 3$*) mais bien plus difficile à démontrer (*preuve très longue et difficile d'une conjecture plus générale par Wiles en 1994*).
- Le « petit » théorème de Fermat est bien plus fondamental que le « grand »...
- La réciproque du petit théorème de Fermat est fausse, et même très fausse (voir le DM sur les nombres de Carmichael).

2.4 Exercices

Généralités

2.1. On a calculé $8! = 40320$. Montrer que les entiers $40322, \dots, 40328$ sont composés.

2.2. Montrer facilement et sans calculatrice que 97 est premier.

2.3. 1. Décomposer 16758.

2. Combien de diviseurs possède ce nombre ?

3. Est-il un carré ?

2.4. 1. Décomposer 121225134276.

2. Est-il un carré ? Si oui, déterminer sa racine carrée.

3. Combien possède-t-il de diviseurs ?

2.5. Trouver le seul nombre premier égal à $x^4 + 4y^4$ où x et y sont des entiers naturels (*résultat dû à Sophie Germain*). On pourra commencer par $x^4 + 4y^4 = (x^2 + 2y^2)^2 - 4x^2y^2 \dots$

2.6. Pour $n \in \{0, \dots, 39\}$, les nombres (*étudiés par Euler*) $n^2 + n + 41$ sont-ils premiers ? Et pour $n = 40$?

Autour du théorème de Gauss

2.7. Montrer qu'un nombre premier est premier avec un entier ssi il ne le divise pas.

2.8. Montrer qu'un nombre premier divise un produit ssi il divise l'un de ses facteurs.

2.9. Montrer que si un nombre premier divise un produit de facteurs premiers alors il est l'un de ces facteurs.

2.10. Montrer que si un entier est premier avec des entiers alors il est premier avec leur produit.

2.11. Pour $0 \leq k \leq n$, on définit $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ (*voir le chapitre 13*). Montrer que si p est premier alors p divise $\binom{n}{p}$.

Cette propriété est à la base de la démonstration par récurrence du petit théorème de Fermat : exercice !

Pgcd, ppcm

2.12. Déterminer le pgcd et le ppcm de 3292907310 et 551034. Vérifier que leur produit donne le produit de ces deux entiers.

2.13. Déterminer les entiers naturels a et b vérifiant $a + b = 171$ et $\text{ppcm}(a, b) = 1716$.

2.14. Déterminer les entiers naturels a et b vérifiant $a^2 + b^2 = 954$ et $\text{ppcm}(a, b) = 135$.

2.15. Montrer que pour tout entier naturel n , la fraction $\frac{5^{n+1} + 6^{n+1}}{5^n + 6^n}$ est irréductible.

On pourra effectuer la division euclidienne du numérateur par le dénominateur puis considérer un diviseur premier de ces deux nombres.

Petit théorème de Fermat

2.16 (preuve du petit théorème de Fermat). Soient a un entier et soit p un nombre premier.

1. Montrer que si a et p ne sont pas premiers entre eux, alors $a^p \equiv a \pmod{p}$.

Ce résultat est la partie triviale du petit théorème de Fermat.

2. On suppose maintenant que a et p sont premiers entre eux.

On pose $E = \{1, 2, \dots, p-1\}$, et on définit $f : E \rightarrow E$ par $f(x) = ax \pmod{p}$.

- (a) Montrer qu'un entier premier avec p possède un inverse modulo p , en utilisant le théorème de Bézout.
- (b) Montrer que f est bien définie, i.e. que $f(x)$ appartient bien à E .
- (c) Montrer que f est une bijection en exhibant sa réciproque.
- (d) En déduire que $\prod_{x \in E} x = \prod_{x \in E} ax \pmod{p}$.
- (e) Montrer que $\prod_{x \in E} x$ est premier avec p en utilisant le théorème de Gauss.
- (f) En déduire $a^{p-1} \equiv 1 \pmod{p}$ (avec p premier et $a \wedge p = 1$).

2.17. Montrer que 17 divise $3^{16} - 1$.

2.18. Montrer que $4^{14} \equiv 1 \pmod{15}$. La réciproque du petit théorème de Fermat est-elle vraie ?

2.19 (algorithme RSA). Soient p et q deux nombres premiers distincts et ≥ 3 . On pose $n = pq$. Soit m un entier vérifiant $0 \leq m < n$.

1. Montrer qu'il existe au moins un entier e premier avec $(p-1)(q-1)$ et vérifiant $1 < e < (p-1)(q-1)$.
2. Montrer qu'il existe un unique entier d vérifiant $ed \equiv 1 \pmod{(p-1)(q-1)}$ (i.e. un inverse modulaire) et $1 \leq d < (p-1)(q-1)$.
3. Montrer que $m^{ed} \equiv m \pmod{n}$ en montrant d'abord cette égalité modulo p et q .

2.20 (mise en oeuvre du cryptage RSA). Une personne A souhaite envoyer un message crypté à une personne B. La transmission du message n'est pas sécurisée (par exemple un mail). B fournit publiquement une clé de cryptage sous forme d'un entier n et un exposant e ; la clé de décryptage sous forme de l'exposant d ne peut pas se déduire de (n, e) en un temps raisonnable. Une telle clé est qualifiée de *publique* et d'*asymétrique*.

Concrètement :

- B choisit secrètement deux (très grands) nombres premiers p et q et publie $n = pq$;

- il choisit un exposant public convenable e (en général petit – souvent 3 – pour simplifier les calculs) ;
- il calcule l'exposant secret d par inversion modulaire ;
- le message à transmettre est découpé en entiers $m < n$;
- A calcule $m' = m^e \bmod n$ et envoie l'entier codé à B ;
- B décode m' par $(m')^d = (m^e)^d = m^{ed} = m \bmod n$.

Un éventuel attaquant indiscret peut capter le message codé m' mais il ne peut calculer (en un temps raisonnable) l'exposant de décodage d . La sécurité essentielle du système (et ce n'est d'ailleurs qu'une conjecture à ce jour) tient en la difficulté de factoriser un très grand entier n type RSA. Les clés s'allongent au fur et à mesure que le matériel informatique progresse...

1. On donne $p = 41$ et $q = 53$. Calculer n ainsi que $(p - 1)(q - 1)$.
2. Montrer que $e = 1427$ est premier avec $(p - 1)(q - 1)$ en utilisant l'algorithme d'Euclide.
3. En déduire l'exposant secret d .
4. Essayer de coder puis décoder 666.

2.21. Comment peut-on utiliser le cryptage RSA pour signer (i.e. authentifier) un message ?

3. Matrices

3.1 Généralités

Définition. Une *matrice* M de taille $n \times p$ est un tableau à deux dimensions de nombres (M_{ij}) où i est la ligne et j la colonne, avec $1 \leq i \leq n$ et $1 \leq j \leq p$.

Par exemple, voici comment est notée et indexée une matrice 3×5 :

$$\begin{pmatrix} M_{11} & M_{12} & M_{13} & M_{14} & M_{15} \\ M_{21} & M_{22} & M_{23} & M_{24} & M_{25} \\ M_{31} & M_{32} & M_{33} & M_{34} & M_{35} \end{pmatrix}.$$

Définition.

- S'il n'y a qu'une seule ligne alors M est une *matrice ligne* ;
- s'il n'y a qu'une seule colonne alors M est une *matrice colonne* ;
- si le nombre de lignes est égal au nombre de colonnes alors M est une *matrice carrée*.

Définition. Deux matrices sont *égales* si elles ont même taille et si leurs éléments respectifs sont égaux.

Définition. Si $M = (M_{ij})$ est une matrice alors $M^t = (M_{ji})$ est sa *matrice transposée*. Si M est de taille $n \times p$ alors M^t est de taille $p \times n$.

Par exemple :

$$M = \begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix} \quad , \quad M^t = \begin{pmatrix} a & d \\ b & e \\ c & f \end{pmatrix}.$$

3.2 Opérations algébriques

3.2.1 Somme

Définition. La *somme* de deux matrices de même taille $n \times p$ est la matrice de taille $n \times p$ formée naturellement comme somme terme à terme. Formellement, $(A + B)_{ij} = A_{ij} + B_{ij}$ avec $1 \leq i \leq n$ et $1 \leq j \leq p$.

Théorème. Soient A , B et C trois matrices de même taille. Alors :

- $A + B = B + A$ (*commutativité*) ;
- $A + O = O + A = A$ (*élément neutre*) où O est la matrice nulle de taille idoine ;
- $A + (B + C) = (A + B) + C$ (*associativité*).

Preuve. Ces résultats sont directement issus des propriétés des ensembles numériques usuels. □

3.2.2 Multiplication par un scalaire

Définition. La *multiplication* d'une matrice par un scalaire est la matrice de même taille formée naturellement comme multiplication de tous ses coefficients. Formellement, si $\lambda \in \mathbb{C}$ alors $(\lambda M)_{ij} = \lambda M_{ij}$.

Théorème. Soient A et B deux matrices de même taille. Soient λ et μ deux scalaires. Alors :

- $\lambda(A + B) = \lambda A + \lambda B$;
- $(\lambda + \mu)A = \lambda A + \mu A$;
- $\lambda(\mu A) = (\lambda\mu)A$.

3.2.3 Produit

Remarque. Il y a de bonnes raisons (liées à la définition des applications linéaires) à la définition suivante, qui peut de prime abord paraître sortie de l'esprit d'un mathématicien fou. Autrement exprimé, cette définition est une manière de rendre compatible le produit matriciel avec la substitution dans les systèmes linéaires (voir plus loin).

Définition. Le *produit* d'une matrice A de taille $n \times p$ par une matrice B de taille $p \times q$ est la matrice C de taille $n \times q$ définie par $C_{ij} = \sum_{k=1}^p A_{ik}B_{kj}$, i.e. le produit de la ligne i de A par la colonne j de B .

Théorème. Soient A , B et C trois matrices de dimensions compatibles. Alors :

- $C(A + B) = CA + CB$ (*distributivité à gauche*) ;
- $(A + B)C = AC + BC$ (*distributivité à droite*).

Remarque. Attention ! l'anneau des matrices n'est pas *intègre*, i.e. il ne vérifie pas le théorème du produit nul.

Voici un exemple tout bête : $\begin{pmatrix} 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = (0)$ et pourtant aucun des deux facteurs n'est une matrice nulle.

3.3 Matrices carrées

Définition. La *matrice identité* de taille n est la matrice carrée de taille n définie par $I_{ij} = 1$ si $i = j$ et $I_{ij} = 0$ si $i \neq j$:

$$I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

Théorème. Si A est une matrice carrée de taille n alors $I_n A = A I_n = A$ (*élément neutre*).

Preuve. C'est un simple calcul.

□

Définition. • Deux matrices carrées A et B de même dimension $n \times n$ sont *inverses* si $AB = BA = I_n$;

- dans ce cas A est *inversible* et son *inverse* B est notée A^{-1} .

Preuve. Nous devons montrer, afin que la définition ci-dessus soit correcte, que l'inverse d'une matrice est unique. Si A possède deux inverses B et C , alors $AB = I_n = AC$. En multipliant à gauche par B , il vient $(BA)B = (BA)C$ i.e. $B = C$. \square

Remarque. • Pour prouver que B est l'inverse de A , vérifier $AB = I_n$ ou $BA = I_n$ suffit.

- S'il existe, l'inverse du produit MN est $N^{-1}M^{-1}$.

Remarque. Un système linéaire à n variables :

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = y_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = y_2 \\ \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n = y_n \end{cases}$$

peut se traduire matriciellement par $AX = Y$, où :

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}, \quad X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}, \quad Y = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}.$$

Résoudre ce système linéaire consiste à trouver X en fonction de Y , i.e. inverser A pour pouvoir écrire $X = A^{-1}Y$.

3.4 Exercices

Calculs élémentaires

3.1. Soient $A = \begin{pmatrix} 1 & 2 & -3 \\ 0 & 1 & 2 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & -1 & -1 \\ 2 & 1 & 0 \end{pmatrix}$.
Calculer $A + B$, $A - B$ et πB .

3.2. Calculer les produits matriciels suivants :

1. $\begin{pmatrix} 1 & 1 \\ 2 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 2 & 0 & 1 \\ 1 & 0 & 2 \end{pmatrix};$

2. $\begin{pmatrix} i & 1 \\ 1 & i \\ 1 & -i \end{pmatrix} \begin{pmatrix} i & 1 & 0 & i \\ 0 & 1 & i & 1 \end{pmatrix};$

3. $\begin{pmatrix} 1 & i & 1 \\ i & 1 & 1 \\ 1 & 1 & i \end{pmatrix} \begin{pmatrix} 1 & 0 & i \\ 0 & i & 1 \\ i & 1 & 0 \end{pmatrix}.$

3.3. On considère les matrices $A = \begin{pmatrix} 1 & 1 & 1 \\ 3 & -2 & 0 \\ 1 & -1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 & -2 \\ 0 & 1 & -3 \\ 1 & x & y \end{pmatrix}$.

1. Quelles valeurs de x et y vérifient $AB = BA$?
2. Que vaut alors AB ?

Inverses et puissances

3.4. Soit $M = \begin{pmatrix} x & 0 & 0 \\ 0 & x & 0 \\ 0 & 0 & x \end{pmatrix}$ i.e. une matrice *diagonale*. Calculer M^n pour n entier naturel.

3.5. Soit $A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$. Établir par récurrence l'expression de A^n , pour n entier naturel.

3.6. On considère la matrice $M = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$.

Calculer M^2 , M^3 et M^4 puis déterminer l'expression de $M^n = M^{4q+r}$ pour n entier naturel.

3.7. Soient $A = \begin{pmatrix} 2 & 3 \\ 2 & 1 \end{pmatrix}$, $D = \begin{pmatrix} -1 & 0 \\ 0 & 4 \end{pmatrix}$, $P = \begin{pmatrix} -1 & 3 \\ 1 & 2 \end{pmatrix}$ et $P' = \frac{1}{5} \begin{pmatrix} -2 & 3 \\ 1 & 1 \end{pmatrix}$.

1. Calculer PP' , D^2 , D^3 et PDP' . (On a effectué une diagonalisation.)
2. En déduire l'expression de A^2 et A^3 , puis de A^n pour $n \in \mathbb{N}$.

3.8. On considère les matrices :

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad , \quad A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad , \quad B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

1. Vérifier rapidement que $A = I + B$.
2. Calculer B^2 puis B^n où n est un entier naturel.
3. Montrer par récurrence que $A^n = I + nB$ pour tout entier naturel n .
4. Montrer que $I - B = A^{-1}$.

3.9. On considère les matrices :

$$I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad , \quad A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \quad , \quad B = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

1. Vérifier rapidement que $A = I + B$.
2. Calculer B^2 , B^3 puis B^n où n est un entier naturel. (On dit que B est *nilpotente*.)
3. On sait que le produit de matrices ne commute pas, en général. La formule du binôme est-elle valable pour une expression matricielle de $(P + Q)^n$?
Qu'en est-il pour $(I + B)^n$?
4. Déterminer l'expression de A^n .
5. Montrer que $A^{-1} = I - B + B^2$.

3.10. Soit A une matrice carrée de taille n . Supposons que $A = I_n - N$ où N est une matrice nilpotente d'ordre k , i.e. $N^{k-1} \neq O_n$ et $N^k = O_n$. Montrer que $A^{-1} = I_n + N + N^2 + \dots + N^{k-1}$.

Divers

3.11. On cherche l'équation de la parabole passant par $P(1; 4)$, $Q(-2; -5)$ et $R(-1; 0)$.

1. Traduire ce problème sous forme d'un système linéaire de 3 équations à 3 inconnues.
2. Convertir ce système en une équation matricielle.
3. Résoudre cette équation matricielle à l'aide d'un logiciel de calcul formel.
4. Vérifier la solution graphiquement.

3.12. À l'aide d'un logiciel de calcul formel, trouver l'intersection des trois plans d'équations $2x + y + z = 8$, $x - 2y - z = -6$ et $x - 3y - z = -4$.

3.13. Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Montrer que si $ad - bc \neq 0$ alors $M^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

3.14. Soit $z = a + ib$ un complexe. Calculer $x' + iy' = z(x + iy)$ puis en déduire la matrice à coefficients réels Z vérifiant $\begin{pmatrix} x' \\ y' \end{pmatrix} = Z \begin{pmatrix} x \\ y \end{pmatrix}$.

3.15. 1. Si $z = x + iy$, quelle est l'image $M'(x' + iy')$ de $M(x + iy)$ par la rotation de centre O et d'angle θ ?

2. Montrer que $\begin{pmatrix} x' \\ y' \end{pmatrix} = R_\theta \begin{pmatrix} x \\ y \end{pmatrix}$, où R_θ est la *matrice de rotation* $\begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$.

3. Calculer R_θ^2 puis établir par récurrence l'expression de R_θ^n . Est-ce étonnant ?

4. *Application.* Calculer sans effort $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^4$ puis $\begin{pmatrix} \sqrt{3} & -1 \\ 1 & \sqrt{3} \end{pmatrix}^{12}$.

3.16. Les quaternions \mathbb{H} (*comme Hamilton*) peuvent se représenter par les *matrices de Pauli* :

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad K = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}.$$

(On prendra garde aux notations ici quelque peu particulières.)

1. Calculer I^2 , J^2 , K^2 , IJ , JK et KI .

2. Calculer $(t1)^2$ puis, si possible à l'aide d'un logiciel de calcul formel, $(xI + yJ + zK)^2$ où x, y, z et t sont des réels.

3. En déduire que si $t1 + xI + yJ + zK = 0$ alors $x = y = z = t = 0$.

4. Un quaternion s'écrit $q = t1 + xI + yJ + zK$. Montrer que cette écriture est unique.

3.17. On définit les matrices de Dirac par :

$$A = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 & 0 & i \\ 0 & 0 & -i & 0 \\ 0 & i & 0 & 0 \\ -i & 0 & 0 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}, \quad D = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

1. Calculer $(xA + yB + zC + tD)^2$ à l'aide, si possible, d'un logiciel de calcul formel.

2. En déduire A^2 , B^2 , C^2 et D^2 .

3. Pour deux matrices quelconques P et Q , a-t-on $(P + Q)^2 = P^2 + Q^2 + 2PQ$?

4. Le *crochet* de deux matrices est $[P, Q] = PQ - QP$.

Calculer les différents crochets des matrices A, B, C et D .

4. Modèles matriciels

4.1 Chiffrement de Hill

On découpe le texte à coder en blocs de trois lettres. Si le nombre de lettres du texte n'est pas un multiple de 3, on complète par une ou deux lettres factices. On utilise la table de correspondance numérique suivante :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Par exemple, le mot CASSOULET est découpé en $B_1 = \begin{pmatrix} 2 \\ 0 \\ 18 \end{pmatrix}$, $B_2 = \begin{pmatrix} 18 \\ 14 \\ 20 \end{pmatrix}$ et $B_3 = \begin{pmatrix} 11 \\ 4 \\ 19 \end{pmatrix}$.

On utilise ensuite une matrice inversible H de taille 3×3 (*la matrice de chiffrement*) pour coder nos blocs de trois lettres via HB_1 , HB_2 et HB_3 , le tout étant pris modulo 26.

4.1. Soit $H = \begin{pmatrix} 1 & 2 & 3 \\ 9 & 7 & 4 \\ 8 & 6 & 5 \end{pmatrix}$.

1. Coder CASSOULET à l'aide de H .
2. Montrer que H est inversible en exhibant son inverse H^{-1} .
3. Peut-on décoder à l'aide de H^{-1} directement ?
4. Montrer que $A = \begin{pmatrix} 23 & 12 & 13 \\ 13 & 17 & 15 \\ 10 & 2 & 3 \end{pmatrix}$ vérifie $AH \equiv I \pmod{26}$.
5. Décoder le message codé à la première question.
6. Comment pourrait-on décoder un long message sans avoir la matrice de chiffrement ?

4.2 Suites récurrentes matricielles linéaires

4.2 (suite de Fibonacci). La suite (f_n) est définie par $f_0 = 0$, $f_1 = 1$ et $f_{n+1} = f_n + f_{n-1}$.

On cherche à exprimer son terme général en fonction de n .

1. Trouver la matrice A vérifiant $\begin{pmatrix} f_{n+1} \\ f_n \end{pmatrix} = A \begin{pmatrix} f_n \\ f_{n-1} \end{pmatrix}$.
2. Montrer que $\begin{pmatrix} f_n \\ f_{n-1} \end{pmatrix} = A^{n-1} \begin{pmatrix} f_1 \\ f_0 \end{pmatrix}$.
3. Soient $P = \begin{pmatrix} 1 + \sqrt{5} & 1 - \sqrt{5} \\ 2 & 2 \end{pmatrix}$ et $Q = \frac{1}{20} \begin{pmatrix} 2\sqrt{5} & 5 - \sqrt{5} \\ -2\sqrt{5} & 5 + \sqrt{5} \end{pmatrix}$. Calculer PQ et QAP .
4. En déduire A^n puis le terme général f_n .

4.3. Soient (u_n) et (v_n) les suites réelles barycentriques définies par $u_0 = 12$ et $u_{n+1} = \frac{u_n + 2v_n}{3}$, $v_0 = 1$ et $v_{n+1} = \frac{u_n + 3v_n}{4}$.

Déterminer les termes généraux et la convergence de ces deux suites.

On pourra utiliser la fonction de jordanisation de Sage, qui permet en particulier de diagonaliser une matrice : `<matrice>.jordan_form(transformation=True)`.

4.3 Suites récurrentes matricielles affines

On vient de voir un exemple de suite récurrente matricielle linéaire $U_{n+1} = AU_n$. On trouve le terme général en calculant A^n et en l'utilisant dans $U_n = A^n U_0$.

Définition. Une suite de matrices de même taille *converge* si chaque élément forme une suite convergente.

4.4 (étude théorique). Soient A une matrice carrée de taille p et B une matrice colonne de taille p . Soit (U_n) une suite de matrices colonnes de taille p définie par $U_{n+1} = AU_n + B$.

1. Supposons qu'une suite constante égale à C vérifie la relation de récurrence. Peut-on expliciter C ?
2. Si une telle suite existe, déterminer le terme général U_n en s'inspirant de la méthode vue dans le cadre des suites récurrentes affines réelles.
3. Montrer que si (A^n) converge alors il en est de même pour (U_n) .

4.5. Soient $A = \begin{pmatrix} 0,3 & 0,2 \\ 0,1 & 0,4 \end{pmatrix}$ et $B = \begin{pmatrix} 12 \\ 0 \end{pmatrix}$.

On définit la suite matricielle (U_n) par $U_0 = \begin{pmatrix} 24 \\ 3 \end{pmatrix}$ et $U_{n+1} = AU_n + B$.

1. Soient $P = \begin{pmatrix} 1 & -2 \\ 1 & 1 \end{pmatrix}$, $D = \begin{pmatrix} 0,5 & 0 \\ 0 & 0,2 \end{pmatrix}$ et $Q = \frac{1}{3} \begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix}$.

Calculer PDQ et QP puis en déduire l'expression de A^n en fonction de n .

2. Exprimer U_n en fonction de n puis étudier la convergence de (U_n) .

4.6. On définit les suites réelles (x_n) et (y_n) par $x_0 = \frac{7}{8}$, $y_0 = \frac{3}{8}$, $x_{n+1} = 6x_n + 3y_n + 4$ et $y_{n+1} = -x_n + 2y_n - 1$.

Déterminer les termes généraux de (x_n) et (y_n) puis étudier leur convergence.

4.4 Modèle d'évolution de Lotka-Volterra

On s'intéresse à l'évolution d'une population de marmottes M_n (les proies) et de renards R_n (les prédateurs), où n représente l'année. Le nombre de marmottes augmente de 10% par an. Il y a $M_n \times R_n$ rencontres possibles ; parmi celles-ci, seules 0,1% ont lieu et se finissent mal pour la marmotte. La population décroît naturellement de 5% par an. Cependant, la nourriture revigore les renards et leur population augmente de 5% du nombre de marmottes croquées.

- 4.7 (modélisation).** 1. Vérifier qu'on a les équations récurrentes d'évolution non linéaires $M_{n+1} = 1,1M_n - 0,001M_nR_n$ et $R_{n+1} = 0,95R_n + 0,0005M_nR_n$.
2. Quelle est la nature de la suite M_n lorsqu'il n'y a pas de renards ? Déterminer son sens de variation et sa limite.
3. Quelle est la nature de la suite R_n lorsqu'il n'y a pas de marmottes ? Déterminer son sens de variation et sa limite.
4. Existe-t-il des populations initiales de R renards et M de marmottes qui rendent leur nombre constant ?

4.8 (étude sur tableur). En 2001, on comptait dans le secteur d'Héry-sur-Ugine 210 marmottes et 50 renards.

1. Étudier l'évolution du nombre de marmottes et de renards jusqu'en 2789.
2. Tracer ces évolutions, d'abord sur une période de 200 ans.
3. Tracer l'évolution conjointe, i.e. les couples (M_n, R_n) .
4. Que se produit-il ?
5. Que se passe-t-il si on change les populations initiales ?

4.9 (étude au voisinage du point d'équilibre). On note $U_n = \begin{pmatrix} M_n \\ R_n \end{pmatrix}$. On se place au voisinage du point d'équilibre $(M; R)$ en effectuant le changement de variable $m_n = M_n - M$ et $r_n = R_n - R$; on suppose donc que m_n et r_n sont petits.

1. Montrer que $m_{n+1} = m_n - 0,1r_n - 0,001m_nr_n$ et $r_{n+1} = r_n + 0,05m_n + 0,0005m_nr_n$.
2. Montrer que ces équations peuvent être raisonnablement approchées par les équations linéaires $m_{n+1} = m_n - 0,1r_n$ et $r_{n+1} = r_n + 0,05m_n$.
3. Traduire matriciellement ce système d'équations et en déduire les expressions de M_n et R_n au voisinage du point d'équilibre.
4. Que se passe-t-il alors lorsque n devient grand ?

4.5 Marches aléatoires

Introduction Imaginons un bonhomme qui se déplace sur les sommets d'un graphe en ayant une probabilité fixée de passer d'un sommet à l'autre. Formalisons :

Une *marche aléatoire* sur un ensemble fini est la donnée :

- d'un ensemble $E = \{x_1, \dots, x_d\}$ d'états ;
- de *probabilités de transition* $\{p_{ij}\}$ entre ces états ;
- d'une *suite aléatoire* $X = (X_n)$ d'états vérifiant $P_{X_n=x_i}(X_{n+1} = x_j) = p_{ij}$ et de répartition initiale aléatoire $\mu_0 = \{\mu_0^1, \dots, \mu_0^d\}$ i.e. $P(X_0 = x_k) = \mu_0^k$.

On s'intéresse donc aux *chaînes de Markov* finies : l'état de X à un temps donné ne dépend que de son état au temps précédent.

Modélisation matricielle Lorsque la marche aboutit à un état x_j , elle vient forcément de l'un des états x_i possibles et la formule des probabilités totales donne :

$$\begin{aligned} P(X_{n+1} = x_j) &= P_{X_n=x_1}(X_{n+1} = x_j)P(X_n = x_1) + \cdots + P_{X_n=x_d}(X_{n+1} = x_j)P(X_n = x_d) \\ &= \sum_{i=1}^d P_{X_n=x_i}(X_{n+1} = x_j)P(X_n = x_i) \\ &= \sum_{i=1}^d p_{ij}P(X_n = x_i) \end{aligned}$$

On est donc amené à poser :

- $M_n = (\mu_n^1 \quad \cdots \quad \mu_n^d)$ la suite de distributions de probabilités, i.e. $\mu_n^k = P(X_n = x_k)$;
- $P = \begin{pmatrix} P_{11} & P_{12} & \cdots & P_{1d} \\ P_{21} & P_{22} & \cdots & P_{2d} \\ \vdots & \vdots & \vdots & \vdots \\ P_{d1} & P_{d2} & \cdots & P_{dd} \end{pmatrix}$ la *matrice de transition*.

La somme de chaque ligne de P vaut 1, tout comme la somme des éléments de M_n (la somme des probabilités des éléments d'une partition vaut 1).

Dans ces conditions, on a l'équation d'évolution stochastique $M_{n+1} = M_n P$. Déterminer l'évolution de la suite (M_n) revient donc à l'étude d'une suite récurrente matricielle linéaire. En particulier, on obtient $M_n = M_0 P^n$ i.e. $P_{X_0=x}(X_n = y) = (P^n)_{xy}$.

Probabilité invariante Un *état stable probabiliste* est une probabilité sur les états de la chaîne conservée à l'étape suivante : les probabilités de présence ne changent pas.

Une *probabilité invariante* est un vecteur π vérifiant $\pi P = \pi$.

On comprend bien l'adjectif « invariante » mais le lien avec un *état physique stable* est plus délicat. Pour éclaircir ce point, on remarque que :

$$\pi P = \pi \Leftrightarrow \sum_y \pi_y P_{yx} = \pi_x \quad \forall x \Leftrightarrow \sum_{y, y \neq x} \pi_y P_{yx} = \pi_x - \pi_x P_{xx} \Leftrightarrow \sum_{y, y \neq x} \pi_y P_{yx} = \pi_x (1 - P_{xx}).$$

Là c'est intéressant car on peut interpréter cette égalité comme $P(X_n \neq x, X_{n+1} = x) = P(X_n = x, X_{n+1} \neq x)$ ce qui signifie que la chaîne a autant de chance de partir de x que d'y arriver, quel que soit l'état x .

Évoquons ensuite le lien entre probabilité invariante et fréquences de visite. Définissons le vecteur aléatoire des fréquences de visite aux différents états x de la chaîne : $Y_n^x = \frac{1}{n} \sum_{k=0}^{n-1} 1_{X_k=x}$.

On passe à l'espérance : $E(Y_n^x) = \frac{1}{n} \sum_{k=0}^{n-1} P(X_k = x) = \left(\frac{1}{n} \sum_{k=0}^{n-1} \mu_0 P^k \right)^x$, ce qui donne vectoriellement : $E(Y_n) = \frac{1}{n} \sum_{k=0}^{n-1} \mu_0 P^k$.

Notons π_n ce vecteur : $\pi_n P = \left(\frac{1}{n} \sum_{k=0}^{n-1} \mu_0 P^k \right) P = \frac{1}{n} \sum_{k=0}^{n-1} \mu_0 P^{k+1} = \pi_n - \frac{1}{n} \mu_0 + \frac{1}{n} \mu_0 P^n$.

Donc si la suite (P^n) converge alors π_n converge et $\lim \pi_n P = \lim \pi_n$ soit finalement $\pi P = \pi$.

Irréductibilité Sur une chaîne finie, il existe toujours une probabilité invariante. L'unicité n'est par contre pas assurée. Par exemple, la chaîne (nombriliste ? conservatrice ?) définie par :



possède une infinité de probabilités invariantes.

Si deux états x et y sont reliés par un *chemin* dont la probabilité est non nulle (i.e. en un certain nombre d'étapes il est possible d'aller de x à y , i.e. $\forall x, y \in E, \exists k \in \mathbb{N}^*, (P^k)_{xy} > 0$) alors x conduit à y . Si x conduit à y et y conduit à x alors les états x et y *communiquent*. Une chaîne dont tous les états communiquent est *irréductible*. Si une chaîne est irréductible alors elle possède une *unique* probabilité invariante.

S'il existe un entier k tel que tous les coefficients de P^k soient strictement positifs (i.e. en k étapes x conduit à y quels que soient les états x et y , i.e. $\exists k \in \mathbb{N}^*, \forall x, y \in E, (P^k)_{xy} > 0$ – noter la différence avec l'irréductibilité simple –, i.e. il existe une puissance $k > 0$ telle que tous les coefficients de P^k sont > 0) alors la chaîne est *fortement irréductible*. Dans ce cas $\lim_{n \rightarrow +\infty} \mu P^n = \pi$, i.e. quelle que soit la répartition de probabilité initiale de la chaîne, ses itérations conduisent à la probabilité invariante.

Périodicité Soient x est un état de la chaîne et $R(x) = \{n \in \mathbb{N}^*, (P^n)_{xx} > 0\}$ l'ensemble des longueurs de chemins qui partent de x pour y revenir. La *période* de x est le pgcd des entiers de $R(x)$.

Si la chaîne est irréductible alors tous ses états ont même période. En effet considérons deux états x et y avec x conduisant à y en m étapes et y conduisant à x en n étapes. Si $r \in R(y)$ alors y conduit à lui-même en r étapes. Ainsi x conduit à lui-même en $m + n$ étapes (via le chemin $x \rightarrow y \rightarrow x$) mais aussi en $m + r + n$ étapes (via le chemin $x \rightarrow y \rightarrow y \rightarrow x$). Par conséquent $m + n \in R(x)$ et $m + r + n \in R(x)$; il en découle que la période de x divise $m + n$ et $m + r + n$ et donc aussi leur différence qui est r . Ceci étant valable quel que soit r dans $R(y)$, on en déduit que $p(x) \leq p(y)$. De même on peut établir que $p(y) \leq p(x)$ et donc que x et y ont même période.

Ceci définit donc la *période* d'une chaîne irréductible. Si cette période vaut 1 alors la chaîne est *apériodique*. Par exemple, s'il existe un état x pour lequel $P_{xx} > 0$ alors la chaîne est apériodique.

La chaîne est fortement irréductible ssi elle est irréductible et apériodique. L'implication directe est facile à établir : supposons la chaîne fortement irréductible d'exposant k ; elle est donc irréductible et il reste à montrer que sa période vaut 1. Choisissons deux états x et y vérifiant $P_{xy} > 0$. On a $(P^{k+1})_{xx} \geq P_{xy}(P^k)_{yx} > 0$. Ainsi k mais aussi $k + 1$ appartiennent à $R(x)$. Ces deux entiers étant premiers entre eux, la période de x vaut 1.

États récurrents et transitoires Un état x est *récurrent* si, en partant de x , la probabilité que le nombre de retours en x soit infini vaut 1. Dans le cas contraire, l'état x est *transitoire*.

Si une chaîne est irréductible alors tous ses états sont soit récurrents soit transitoires. Or nous considérons des chaînes finies : il y existe donc au moins un état récurrent (c'est le *principe des tiroirs*). Par conséquent une chaîne finie et irréductible est donc récurrente.

La *matrice potentielle* de la chaîne est $U = I + P + P^2 + \dots + P^n + \dots$. Ses éléments peuvent être finis ou infinis. Le nombre U_{xy} représente le nombre moyen de visites de la chaîne à l'état y en partant de l'état x . En effet, le nombre moyen de visites à l'état y en partant de x en n étapes exactement est $(P^n)_{xy}$.

On vérifie facilement que $U = I + P(I + P + P^2 + \dots) = I + PU$. Si la matrice $I - P$ est inversible alors $U = \frac{I}{I - P}$. Le résultat est à mettre en relation avec la somme des termes

d'une suite géométrique : $1 + q + q^2 + \dots + q^n = \frac{1 - q^{n+1}}{1 - q}$, qui tend vers $\frac{1}{1 - q}$ si $-1 < q < 1$.

Si $U_{xx} = +\infty$ alors l'état x est récurrent et si $U_{xx} < +\infty$ alors il est transitoire.

Assez intuitivement, si x conduit à y mais y ne conduit pas à x alors x est un état transitoire.

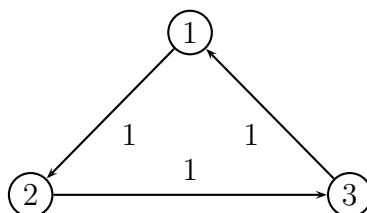
Théorème ergodique Si la chaîne est irréductible (et donc récurrente) et de probabilité invariante π alors $\pi_x = \lim_{n \rightarrow +\infty} \frac{1}{n} \sum_{k=0}^{n-1} 1_{X_k=x} = \lim_{n \rightarrow +\infty} \frac{1}{n} \sum_{k=0}^{n-1} (P^k)_{yx}$ i.e. quel que soit l'état y de départ de la chaîne, le nombre moyen de visites à l'état x tend vers la probabilité invariante de l'état x .

De plus, si T_x est l'instant du premier retour en x en partant de x alors $\pi_x = \frac{1}{E(T_x)}$.

(Rappel : si la chaîne est apériodique alors $\lim_{n \rightarrow +\infty} (P^n)_{yx} = \pi_x$ quel que soit l'état y initial.)

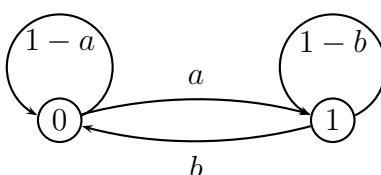
Exercices

4.10. Soit la chaîne :



1. La chaîne est-elle irréductible ?
2. Montrer que la suite (P^n) ne converge pas.
3. La chaîne est-elle apériodique ?

4.11. Un bit est transmis à travers un réseau. À chaque relais, ce bit est transmis avec une probabilité d'erreur égale à a pour un passage de 0 à 1 et égale à b pour l'inverse. On note X_n le résultat de ce bit au n -ème relais. On suppose que les relais sont indépendants et donc que les erreurs commises aussi.



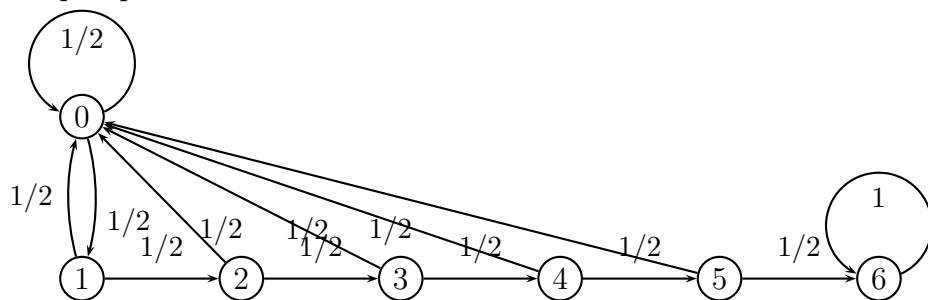
1. Donner la matrice de transition P .
2. On note $g_n = P(X_n = 0)$. Montrer que $g_{n+1} = (1 - a - b)g_n + b$.
3. En déduire que $g_n = (1 - a - b)^n \frac{a}{a+b} + \frac{b}{a+b}$ si le bit initial est 0.
4. Déterminer la limite de g_n .

4.12. Jasper le hamster vit dans une cage. Il peut dormir, courir dans sa roue ou manger ; il change d'activité toutes les minutes. Quand il dort, il a 9 chances sur 10 de ne pas se réveiller la minute suivante ; lorsqu'il se réveille, il a une même probabilité d'aller manger ou courir. Après avoir mangé, il a 3 chances sur 10 de partir courir et il ne continue jamais à grignoter. Une fois qu'il a couru, il a 8 chances sur 10 de retourner dormir ; sinon, il continue à courir.

1. Quelle quantité de paracétamol devra ingérer un élève de spé maths afin de faire disparaître la forte céphalée issue de la lecture de l'énoncé ?
2. Donner la matrice de transition P de cette chaîne.
3. La chaîne est-elle irréductible ? apériodique ?
4. Calculer une bonne approximation de l'état stable à l'aide d'une calculatrice ou d'un logiciel de calcul.
5. Déterminer cet état stable par résolution exacte de l'équation d'invariance à l'aide d'un logiciel de calcul formel.
6. Vérifier la cohérence des réponses aux deux questions précédentes.

4.13. On lance 100 fois une pièce ; on note 1 pour « pile » et 0 pour « face ». On souhaite calculer la probabilité p d'obtenir au moins une suite de 6 « pile » consécutifs.

1. Simuler un grand nombre N fixé de 100 tirages aléatoires de 0 et de 1 et calculer la fréquence empirique d'obtention d'au moins 6 « pile » consécutifs.
2. Quel intervalle de confiance pour p au niveau de 95% peut-on donner ?
3. Expliquer à quoi peut servir la chaîne suivante :



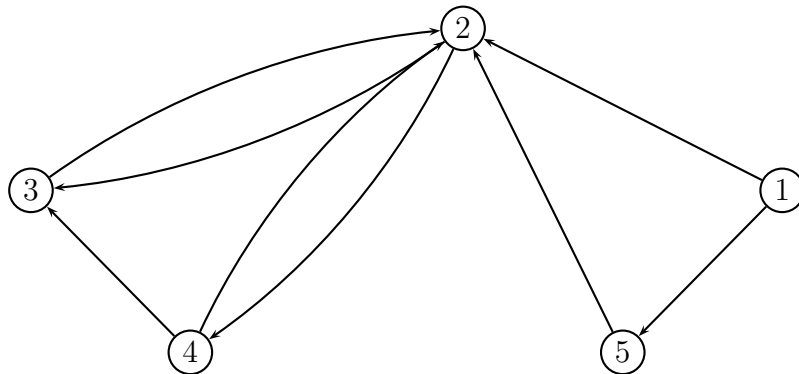
4. Modéliser matriciellement cette chaîne.
5. Calculer P^{100} et répondre au problème posé.
6. L'état 6 est un *cimetière*. La chaîne est-elle irréductible ?

4.14. On considère une enceinte hermétique possédant deux compartiments A et B séparés par une plaque. On injecte 2 molécules d'un gaz dans la compartiment A puis on ôte la séparation de A et B. Les molécules migrent alors entre les deux compartiments aléatoirement : à chaque étape, une molécule prise au hasard dans A+B passe dans l'autre compartiment.

1. Dessiner le graphe probabiliste des états.
2. Donner la matrice de transition P .
3. (a) Donner le vecteur des états probabilistes initial U_0 .
 (b) Déterminer P^0, P^1, P^2, P^3 puis P^n pour tout entier naturel n .
 (c) En déduire l'expression de U_n pour tout entier naturel n .
 (d) La suite (U_n) converge-t-elle ?
 (e) Montrer que le processus possède un état stable $\pi = (x \ y \ z)$.
4. Soit T_n le temps de retour à l'état initial en $2n$ étapes.
 (a) Montrer que $P(T_n = 2k + 1) = 0$ et que $P(T_n = 2k) = \frac{1}{2^k}$.
 (b) Donner la loi de T_n .
 (c) En déduire que $E(T_n) = \sum_{k=1}^n \frac{k}{2^{k-1}}$.
 (d) Montrer que $E(T_n) = 4 - \frac{n+2}{2^{n-1}}$. Quelle est sa limite lorsque n tend vers $+\infty$?

Lorsque le nombre de molécules introduites vaut N très grand, $\lim E(T_n) = 2^N$ est extrêmement grand ; ceci explique pourquoi ce système physique est réversible en théorie mais pas en pratique.

4.15. On considère cinq pages web concernant le sujet « je suis content de faire le dernier exercice de l'année sans mon professeur ». Sur chaque page, des liens pointent vers d'autres pages, symbolisés par le graphe suivant :



1. On suppose qu'un internaute qui arrive sur une de ces pages suit les liens proposés de façon équiprobable. Donner la matrice de transition associée à ce graphe probabiliste.
2. On suppose que l'internaute est initialement sur la page 1. Quelles sont les probabilités qu'il arrive sur les différentes pages après 1 lien ? 10 liens ? 50 liens ? 100 liens ?
3. Quelle est la page qui a la plus grande probabilité d'être visitée après 100 clics ?
4. Quelle semble être la distribution $\tilde{\pi}$ de probabilités limite en partant de la page 1 ? Préciser la conjecture en identifiant les nombres décimaux obtenus sous forme fractionnaire.
5. Montrer que $\tilde{\pi}P = \tilde{\pi}$ et qu'ainsi $\tilde{\pi}$ est un état stable.
6. Montrer plus précisément que c'est le seul état stable en résolvant l'équation $XP = X$ et en retrouvant ces valeurs.
7. Quelles sont les notes de pertinence de nos 5 pages web ?

Partie III

Devoirs à la maison – Tronc commun

DM 1. Formules trigonométriques

On rappelle les trois formules trigonométriques fondamentales :

$$\begin{cases} \cos^2 x + \sin^2 x = 1 ; \\ \sin(x + y) = \sin x \cos y + \cos x \sin y ; \\ \cos(x + y) = \cos x \cos y - \sin x \sin y. \end{cases}$$

1.1 Formules courantes

★

Montrer, en utilisant ces relations, les formules supplémentaires suivantes :

1. $\sin(x - y) = \sin x \cos y - \cos x \sin y ;$
2. $\cos(x - y) = \cos x \cos y + \sin x \sin y ;$
3. $\cos 2x = \cos^2 x - \sin^2 x = 2 \cos^2 x - 1 = 1 - 2 \sin^2 x ;$
4. $\sin 2x = 2 \sin x \cos x ;$
5. $\cos x \cos y = \frac{1}{2}(\cos(x + y) + \cos(x - y)) ;$
6. $\sin x \sin y = \frac{1}{2}(\cos(x - y) - \cos(x + y)) ;$
7. $\sin x \cos y = \frac{1}{2}(\sin(x + y) + \sin(x - y)).$

Toutes ces formules sont à connaître absolument.

1.2 Formules de changement de variable

★

★

On pose $t = \tan \frac{x}{2}$. Montrer que $\cos x$, $\sin x$ et $\tan x$ s'expriment en fonction de t :

1. $\cos x = \frac{1 - t^2}{1 + t^2} ;$
2. $\sin x = \frac{2t}{1 + t^2} ;$
3. $\tan x = \frac{2t}{1 - t^2}.$

DM 2. Relativité très restreinte

2.1 Cône de lumière de Minkowski

★

On se place dans l'espace affine euclidien, muni d'un repère orthonormé $(O; \vec{u}, \vec{v}, \vec{w})$, représentant un espace vide n'étant soumis à aucun champ de force. Les mobiles considérés dans ce problème se déplacent dans le plan $(O; \vec{u}, \vec{v})$, et on place l'axe des temps sur la demi-droite $[O, \vec{w})$ (c'est-à-dire que $t \geq 0$).

Soit $P(x, y, t)$ un photon mobile de coordonnées (x, y) dépendant d'un temps $t \geq 0$, se trouvant à l'origine à l'instant $t = 0$ et se déplaçant dans le plan $(O; \vec{u}, \vec{v})$. On note c la vitesse de la lumière.

1. Quelle est la vitesse de P ?
2. Établir la relation de Minkowski $x^2 + y^2 - c^2 t^2 = 0$ pour ce photon $P(x, y, t)$.
3. Quelle figure géométrique \mathcal{C} est définie par l'équation précédente (ne pas oublier $t \geq 0$) ? Faire un dessin schématique.
4. Quelle inéquation décrivent les coordonnées de l'ensemble des points intérieurs à \mathcal{C} ?
5. Soit maintenant $M(x_M, y_M, t)$ un mobile quelconque, placé à l'origine au temps $t = 0$. Où se situe nécessairement le point M par rapport à \mathcal{C} ?

2.2 Produit de Lorentz

★

★

Certains vecteurs (rapportés à l'origine) sont situés à l'intérieur de \mathcal{C} (appelé *cône de lumière*). On dit que ces vecteurs sont de *type temps*. Soient $\vec{a}(x, y, t)$ et $\vec{a}'(x', y', t')$ deux vecteurs de type temps. On définit leur *produit lorentzien* par $\langle \vec{a}, \vec{a}' \rangle = xx' + yy' - c^2 tt'$.

1. Montrer que $\langle \vec{a}, \vec{a} \rangle \leq 0$.
2. Soit $\lambda > 0$. Montrer que $\lambda \vec{a}$ et $\vec{a} + \vec{a}'$ sont encore de type temps.
3. En déduire que \mathcal{C} est convexe. Est-ce étonnant graphiquement ?

DM 3. Modèle logistique discret

3.1 Présentation du problème



3.1.1 Système itératif

Considérons une espèce animale dont les générations successives ne se chevauchent pas. On peut penser par exemple aux papillons de nuit ou à des espèces d'insectes qui vivent une année et subsistent à l'état d'oeuf pendant l'hiver.

Notons $p(n)$ la population à la n -ième génération. Supposons que l'évolution de cette population ne dépende que de l'effectif de la génération précédente. Mathématiquement, ceci signifie qu'il existe une fonction f telle que

$$p(n+1) = f(p(n)).$$

Cette équation d'évolution est appelée *système itératif*.

3.1.2 Modèle linéaire

Dans ce premier type de modèle, le système itératif est donné par

$$p(n+1) = (1 + \alpha)p(n)$$

où α est un réel strictement positif (sinon l'espèce s'éteint rapidement, *réfléchir pourquoi*). On reconnaît une suite géométrique de raison $(1 + \alpha)$, et on obtient clairement $p(n) = (1 + \alpha)^n p(0)$.

La population croît ainsi exponentiellement. Ceci n'est donc qu'un modèle idéalisé, dans lequel on ne tient pas compte de la surpopulation ou des maladies par exemple.

3.1.3 Modèle logistique

Supposons qu'il y ait un effectif stable p_s de la population, c'est-à-dire un effectif supportable par l'environnement. Supposons de plus que le taux de fertilité dépende linéairement de la différence entre la population effective et la population stable.

Un modèle répondant à ces conditions est donné par

$$p(n+1) = \left(1 + \alpha \frac{p_s - p(n)}{p_s}\right) p(n).$$

Il se révèle plus pratique de prendre p_s comme unité de population.

On pose donc $q(n) = \frac{p(n)}{p_s}$. La relation de récurrence devient alors

$$q(n+1) = (1 + \alpha)q(n) - \alpha q(n)^2.$$

Cette équation d'évolution est appelée *modèle logistique*.

3.2 Étude partielle du modèle logistique

★
★

3.2.1 $\alpha = 1$

1. On pose $x(n) = 1 - q(n)$. Montrer que $x(n+1) = x(n)^2$.
2. Exprimer $q(n)$ en fonction de $x(0)$ et de n .
3. En déduire, selon les valeurs de $x(0)$, le comportement de $q(n)$.
4. En revenant au sens concret des quantités utilisées, reprendre la réponse précédente.

3.2.2 $\alpha = 3$

1. On pose $x(n) = 2 - 3q(n)$. Montrer que $x(n+1) = x(n)^2 - 2$.
2. On pose $x(n) = 2 \cos \theta(n)$. Montrer que $\theta(n+1) = 2\theta(n)$.
3. On suppose que $q(0) = \frac{1}{5}$. Représenter quelques termes de la suite $x(n)$.
4. Peut-on apparemment prévoir son comportement ?

Notons que si l'on marque 1 lorsque $x(n) > 0$ et 0 lorsque $x(n) < 0$, on génère une suite pseudo-aléatoire de 0 et de 1.

3.2.3 Cas général

On pose $x(n) = \frac{1+\alpha}{2} - \alpha q(n)$.

Montrer qu'il existe un nombre c (que l'on déterminera en fonction de α) vérifiant

$$x(n+1) = x(n)^2 + c.$$

Ceci conduit à des études vraiment difficiles, qui amènent à observer des comportements caotiques. La valeur de c est cruciale ; lorsque c est complexe, on peut obtenir de magnifiques dessins fractals dans le plan, dont les plus connus sont les ensembles de Julia et Mandelbrot.

DM 4. Suites et nombre d'or

4.1 Le nombre d'or



1. Résoudre dans \mathbb{R} l'équation $x^2 - x - 1 = 0$. On note ϕ la solution positive, appelée *nombre d'or*. Donner sa valeur exacte puis une valeur approchée au millièm.

2. Prouver les égalités : $\phi^2 = \phi + 1$; $\phi = 1 + \frac{1}{\phi}$; $\phi = \sqrt{1 + \phi}$; $\phi = \frac{\phi^2 + 1}{2\phi - 1}$.

On évitera bien des calculs en se souvenant de l'équation de la question précédente... Les trois dernières égalités montrent que ϕ reste fixe par trois fonctions différentes. Ceci amène la définition de trois suites récurrentes, qui convergent vers ce point fixe. On en étudie une ci-après.

4.2 La suite (a_n)



On pose $a_0 = 2$ et $a_{n+1} = 1 + \frac{1}{a_n}$ pour $n \in \mathbb{N}$.

1. Montrer par récurrence que $\frac{3}{2} \leq a_n \leq 2$ pour tout n .

2. Montrer que $|a_{n+1} - \phi| \leq \frac{4}{9}|a_n - \phi|$ pour tout $n \geq 1$.

On pourra utiliser l'égalité $\phi = 1 + \frac{1}{\phi}$.

3. En déduire, par récurrence, que pour $n \geq 1$ que $|a_n - \phi| \leq \left(\frac{4}{9}\right)^{n-1} |a_1 - \phi|$, puis que

$$|a_n - \phi| \leq \left(\frac{4}{9}\right)^n.$$

4. Montrer que (a_n) converge vers ϕ .

On rappelle le théorème d'encadrement : une suite encadrée par deux suites convergeant vers la même limite est convergente, et sa limite est celle des deux suites encadrantes.

5. Déterminer un entier n_a à partir duquel on a $|a_n - \phi| \leq 10^{-6}$.

4.3 Puissances du nombre d'or

★

On rappelle que le nombre d'or ϕ vérifie $\phi^2 = \phi + 1$.

La *suite de Fibonacci* est définie par $f_0 = 0$, $f_1 = 1$ et $f_{n+1} = f_n + f_{n-1}$.

1. Calculer f_0, \dots, f_9 .
2. Réduire les puissances ϕ^2, \dots, ϕ^6 sous la forme $a\phi + b$. Que peut-on conjecturer sur ϕ^n ?
3. Vérifier cette conjecture par récurrence.

4.4 Suite de Fibonacci

★

Soit (f_n) la suite définie par $f_0 = 0$, $f_1 = 1$ et $f_{n+2} = f_{n+1} + f_n$ (suite de Fibonacci).

★

Dans ce qui suit, $n \geq 1$. Soit (φ_n) la suite définie par $\varphi_n = \frac{f_{n+1}}{f_n}$.

★

1. Calculer les 10 premiers termes de (f_n) et (φ_n) sur un tableur. Que peut-on conjecturer ?
2. Montrer rapidement que (f_n) est entière, strictement positive ($n > 0$) et strictement croissante.

En déduire que (f_n) diverge vers $+\infty$.

3. Montrer que $\varphi_{n+1} = 1 + \frac{1}{\varphi_n}$. Montrer que le nombre d'or ϕ est la seule limite possible de la suite (φ_n) .

4. Montrer que $f_{n+1} - \phi f_n = \frac{(-1)^n}{\phi^n}$ puis que $\varphi_n - \phi = \frac{(-1)^n}{f_n \phi^n}$.

5. En déduire que (φ_n) converge vers ϕ .

DM 5. Études de suites

5.1 Mensualités d'un emprunt

★
★ David souhaite emprunter un montant de C_0 euros afin de refaire le toit de sa maison. La banque accepte de lui prêter cette somme, qu'il devra rembourser à un taux mensuel de t (avec $0 < t < 1$) sur n mois. Chaque mois, David va rembourser les intérêts dus pendant un mois au début du mois suivant ainsi qu'une partie du capital emprunté. Le remboursement se fait en versant chaque mois une traite fixe égale à R . Au début du mois n° k , David doit encore rembourser un capital de C_k .

1. Établir que $C_{k+1} = (1+t)C_k - R$ (on obtient donc une suite arithmético-géométrique).
2. Montrer que $C_k = (1+t)^k \left(C_0 - \frac{R}{t} \right) + \frac{R}{t}$.
3. Pourquoi C_n est-il nul ? En déduire que $R = \frac{t(1+t)^n}{(1+t)^n - 1} C_0$.
4. Une somme S placée au taux mensuel t doit rapporter autant que placée à un taux annuel T . Montrer que $(1+t)^{12}S - S = (1+T)S - S$ puis en déduire t .
5. *Application.* Quelle mensualité doit rembourser David s'il souhaite emprunter 80 000 euros sur 15 ans à 4% annuels ?

5.2 Algorithme de Babylone

- ★
★ Soient $a > 0$ et (u_n) la suite définie par $u_0 > \sqrt{a}$ et $u_{n+1} = \frac{1}{2} \left(u_n + \frac{a}{u_n} \right)$.
1. Étudier sur \mathbb{R}_+^* la fonction définie par $f(x) = \frac{1}{2} \left(x + \frac{a}{x} \right)$.
 2. Étudier le signe de $f(x) - x$ pour $x > 0$.
 3. Montrer que $\sqrt{a} < u_{n+1} < u_n$ pour tout n .
 4. En déduire que (u_n) est minorée par \sqrt{a} (*donc* > 0 et bien définie), décroissante et convergente. Calculer ensuite sa limite.
 5. On pose $v_n = \frac{u_n - \sqrt{a}}{u_n + \sqrt{a}}$. Exprimer v_{n+1} en fonction de v_n et en déduire que $v_n = v_0^{2^n}$.
 6. Montrer que $0 \leq u_n - \sqrt{a} \leq 2u_0v_0^{2^n}$ et en déduire la limite de (u_n) .
 7. *Application.* Calculer grâce à un tableur quelques termes de la suite (u_n) pour $a = 2$ et $u_0 = 2$. La convergence est-elle rapide ? En quoi la formule de la question précédente le confirme ?

5.3 Moyenne arithmético-géométrique



Soient (u_n) et (v_n) les deux suites définies par $u_0 = 1$, $v_0 = 2$, $u_{n+1} = \sqrt{u_n v_n}$ (*moyenne géométrique*) et $v_{n+1} = \frac{u_n + v_n}{2}$ (*moyenne arithmétique*). On admet que (u_n) et (v_n) sont strictement positives (*évident par récurrence*).

1. Observer le comportement de ces deux suites sur un tableur. Quelles conjectures peut-on émettre ?
2. Montrer que $u_n \leq v_n$ quel que soit $n \in \mathbb{N}$.
3. Montrer que (u_n) est croissante et (v_n) décroissante.
4. En déduire que (u_n) et (v_n) convergent.
5. Montrer que ces deux suites ont même limite ℓ (*appelée moyenne arithmético-géométrique*) et donc sont adjacentes.
6. Montrer que $v_{n+1} - u_{n+1} = \frac{1}{2} \frac{(v_n - u_n)^2}{(\sqrt{u_n} + \sqrt{v_n})^2}$. En déduire que $v_{n+1} - u_{n+1} < \frac{1}{8}(v_n - u_n)^2$.
7. Montrer que $v_n - u_n \leq \frac{8}{8^{2^n}}$.

DM 6. Classes de fonctions continues

6.1 Résolution d'une équation fonctionnelle

★

Soit $f : \mathbb{R} \longrightarrow \mathbb{R}$ une fonction continue vérifiant l'équation fonctionnelle

$$f(x + y) = f(x) + f(y)$$

pour tous réels x et y .

1. Montrer que $f(0) = 0$ puis en déduire que f est impaire.
2. (a) Montrer par récurrence que $f(nx) = nf(x)$ pour tout réel x et tout entier naturel n .
(b) Montrer que ce résultat persiste si n est un entier négatif.
3. Soit $r = \frac{p}{q}$ un rationnel, avec p et q relatifs et $q \neq 0$.

Montrer que $f(r) = rf(1)$.

On prendra garde à n'utiliser que des opérations avérées ; on sait pour l'instant uniquement que $f(x) = xf(1)$ si x est entier.

4. Soit x un réel.
(a) Décrire une suite simple de rationnels convergeant vers x .
On pourra se souvenir qu'un réel est un « nombre à virgule »...
(b) Montrer que $f(x) = xf(1)$.

5. En déduire que f est une fonction linéaire.

Les fonctions vérifiant $f(x + y) = f(x) + f(y)$ sont donc les fonctions linéaires. Ce résultat sera utile lors de l'étude du couple exponentielle-logarithme.

6.2 Fonctions contractantes

★

★

★

Soit $f : [a; b] \longrightarrow [a; b]$ vérifiant

$$|f(x) - f(y)| < |x - y|$$

pour tous réels x et y de $[a; b]$ distincts.

1. Montrer que f est continue sur $[a; b]$.
On reviendra ici à la définition.
2. Montrer que f possède au moins un point fixe dans $[a; b]$.
On pourra penser que le théorème des valeurs intermédiaires n'est pas loin...
3. Montrer que ce point fixe est unique.
On pourra raisonner par l'absurde.

6.3 Isométries de la droite réelle

★
★
★ Soit \mathcal{I} l'ensemble des *isométries* de \mathbb{R} , i.e. l'ensemble des fonctions $f : \mathbb{R} \rightarrow \mathbb{R}$ vérifiant $|f(x) - f(y)| = |x - y|$ quels que soient les réels x et y .

1. Soit $f \in \mathcal{I}$.

(a) Montrer que f est continue.

(b) Montrer que f est *injective*, i.e. qu'un réel possède au plus un antécédent par f .

(c) Montrer que f est strictement monotone.

On pourra utiliser ici le théorème des valeurs intermédiaires.

2. Déterminer l'ensemble \mathcal{I} .

On pourra choisir $x < y$ et discuter de l'équation initiale suivant la monotonie de f .

6.4 Fonctions continues commutant

★
★ Soient f et g deux fonctions continues sur le segment $I = [0; 1]$ telles que $f \circ g = g \circ f$, i.e. f et g *commutent*.

On va montrer qu'il existe alors $\ell \in I$ vérifiant $f(\ell) = g(\ell)$, i.e. les courbes de f et g se touchent. Raisonons par l'absurde et supposons que $f(x) \neq g(x)$ pour tout $x \in I$. Soit a un point fixe de f . (*On rappelle que toute fonction continue de I dans I possède au moins un point fixe.*)

1. Montrer que $h = f - g$ est de signe constant. En déduire que $f > g$ ou $f < g$.

2. Soit (u_n) la suite définie par $u_0 = a$ et $u_{n+1} = g(u_n)$.

(a) Montrer que (u_n) est bornée.

(b) Montrer que u_n est un point fixe de f pour tout $n \in \mathbb{N}$.

(c) Montrer que (u_n) est monotone en utilisant la question 1.

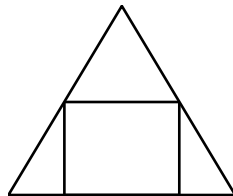
(d) En déduire que (u_n) converge vers un réel ℓ .

3. Montrer par continuité que $f(\ell) = \ell$ et $g(\ell) = \ell$.

4. Conclure.

DM 7. Géométrie et optimisation

7.1 Aire maximale



Soit un rectangle inscrit, comme sur la figure ci-dessus, dans un triangle isocèle dont la base et la hauteur mesurent 12 et 10 respectivement. Le but est de calculer pour quelle largeur du rectangle son aire est maximale.

Faire un dessin sous GeoGebra, conjecturer le résultat puis le prouver.

7.2 Distance d'un point à une parabole



Dans un repère orthonormal, on considère la parabole \mathcal{P} d'équation $y = x^2$ et le point A de coordonnées $(3; 0)$. Le but est de calculer la distance de A à \mathcal{P} .

Faire un dessin sous GeoGebra, conjecturer le résultat puis le prouver analytiquement.

7.3 Tangente commune



Montrer que la parabole \mathcal{P} d'équation $y = x^2$ et l'hyperbole \mathcal{H} d'équation $y = \frac{1}{x}$ possèdent une unique tangente commune. Réaliser conjointement le dessin correspondant sous GeoGebra.

7.4 Photographie de la statue de la Liberté



On veut déterminer la distance x à laquelle on doit placer un appareil photo pour prendre la statue de la Liberté sous un angle θ maximal. On admet que $\theta \in \left]0; \frac{\pi}{2}\right[$. L'appareil photo est à 1,5 m du sol, le piédestal et la statue mesurent au total 45 m.

1. Faire un dessin à la main.
2. Montrer que θ est maximal lorsque $\tan \theta$ l'est.
3. Montrer que $\tan(a - b) = \frac{\tan a - \tan b}{1 + \tan a \tan b}$.
4. Exprimer $\tan \theta$ en fonction de x .
5. Déterminer x pour que $\tan \theta$ soit maximal.

DM 8. Études de fonctions

8.1 Une fonction rationnelle



On considère la fonction f définie sur \mathbb{R} par $f(x) = \frac{x^3 - 4}{x^2 + 1}$.

On note \mathcal{C} sa courbe représentative dans un repère orthonormal d'unité 1 cm.

1. On pose la fonction auxiliaire $g(x) = x^3 + 3x + 8$.
 - (a) Étudier le sens de variation de g .
Montrer que l'équation $g(x) = 0$ admet sur \mathbb{R} une unique solution α dont on donnera un encadrement d'amplitude 0, 1.
 - (b) Préciser le signe de $g(x)$ selon les valeurs de x .
2.
 - (a) Calculer $f'(x)$ puis étudier le sens de variation de f .
 - (b) Étudier les limites de f en $+\infty$ et $-\infty$, puis dresser le tableau de variation de f .
3.
 - (a) Montrer qu'il existe des réels a, b, c et d tels que $f(x) = ax + b + \frac{cx + d}{x^2 + 1}$.
On procèdera par identification, mais on vérifiera par division euclidienne.
 - (b) En déduire que \mathcal{C} admet une asymptote oblique Δ .
Étudier la position de \mathcal{C} par rapport à Δ .
Vérifier que \mathcal{C} rencontre Δ en un unique point A .
4. Déterminer les abscisses des points B, B' de \mathcal{C} admettant une tangente parallèle à Δ .
5.
 - (a) Vérifier que $f(\alpha) = \frac{3}{2}\alpha$, puis en déduire une valeur approchée de $f(\alpha)$.
 - (b) Faire un dessin de \mathcal{C} , contenant les éléments vus dans ce problème.
On pourra utiliser un grapheur.

8.2 Développements limités du sinus et du cosinus

★
★

8.2.1 Encadrements

Soit x un réel positif. Établir successivement les inégalités suivantes :

1. $\sin x \leq x$;
2. $1 - \frac{x^2}{2} \leq \cos x$;
3. $x - \frac{x^3}{6} \leq \sin x$;
4. $\cos x \leq 1 - \frac{x^2}{2} + \frac{x^4}{24}$.

On pourra étudier les différences des quantités comparées en calculant leurs dérivées et en dressant leurs tableaux de variation. On en déduira un encadrement de $\sin x$ et un autre de $\cos x$.

8.2.2 Applications

On utilisera la question précédente.

1. (a) Donner un encadrement de $\sin 0,2$ et de $\cos 0,2$.
(b) Déterminer les 17 premières décimales de $\cos(0,0001)$.
2. (a) Étudier la limite en 0 de $\frac{x - \sin x}{x^2}$.
(b) Étudier la limite en 0 de $\frac{1 - \cos x}{x^2}$.
3. Soit f la fonction définie sur \mathbb{R} par $f(x) = \frac{\sin x}{x}$ si $x \neq 0$ et par $f(0) = 1$.
(a) Tracer \mathcal{C}_f entre -1 et 1 .
On pourra utiliser ici un grapheur.
(b) Montrer que $\lim_{x \rightarrow 0} \frac{\sin x}{x} = 1$.
(c) Étudier la dérivabilité de f en 0.

DM 9. Fonctions trigonométriques

9.1 Fonction arctangente



On admet l'existence d'une fonction f , définie et dérivable sur \mathbb{R} , et vérifiant

$$f(0) = 0 \quad \text{et} \quad f'(x) = \frac{1}{1+x^2}.$$

1. (a) Montrer que la fonction $g : x \mapsto f(x) + f(-x)$ est dérivable, puis calculer sa dérivée.
(b) Calculer $g(0)$. En déduire que f est impaire.
2. (a) Montrer que la fonction $h : x \mapsto f(x) + f\left(\frac{1}{x}\right)$ est dérivable sur \mathbb{R}_+^* , puis calculer sa dérivée.
On rappelle que $[f(u)]' = u'f'(u)$.
(b) En déduire l'existence d'une constante c telle que $f(x) = c - f\left(\frac{1}{x}\right)$ pour $x > 0$.
(c) Prouver que $\lim_{x \rightarrow +\infty} f(x) = c$.
3. On considère la fonction u , définie sur $\left]-\frac{\pi}{2}; \frac{\pi}{2}\right[$ par $u(x) = \tan x$.
(a) Montrer que la fonction $\varphi : x \mapsto (f \circ u)(x) - x$ est dérivable sur $\left]-\frac{\pi}{2}; \frac{\pi}{2}\right[$, puis calculer sa dérivée.
(b) Calculer $\varphi(0)$. En déduire que pour tout x de $\left]-\frac{\pi}{2}; \frac{\pi}{2}\right[$, on a $f(\tan x) = x$.
(c) Calculer les valeurs exactes de $f(1)$, $f(\sqrt{3})$, $f\left(\frac{1}{\sqrt{3}}\right)$.
Donner ensuite la valeur exacte de c .
4. (a) Étudier le sens de variation de f sur \mathbb{R}_+ et dresser son tableau de variation.
(b) Tracer la courbe de f . On précisera les asymptotes et la tangente à l'origine.

9.2 Une somme de Fourier

★
★
★

Préliminaire. Prouver que $\cos a + \cos b = 2 \cos \frac{a+b}{2} \cos \frac{a-b}{2}$, à partir des formules usuelles fondamentales :

$$\begin{cases} \cos^2 a + \sin^2 a = 1 ; \\ \sin(a+b) = \sin a \cos b + \cos a \sin b ; \\ \cos(a+b) = \cos a \cos b - \sin a \sin b. \end{cases}$$

Considérons le signal f , défini sur \mathbb{R} par

$$\begin{cases} f(t) = 1 \text{ si } 0 \leq t < 0,5 \\ f(t) = -1 \text{ si } 0,5 \leq t < 1 \\ f \text{ est } 1\text{-périodique} \end{cases}$$

Définissons ensuite, pour $n \in \mathbb{N}^*$, les fonctions définies sur \mathbb{R} par

$$S_n(t) = \frac{4}{\pi} \sum_{k=0}^{n-1} \frac{1}{2k+1} \sin[(2k+1)2\pi t].$$

1. Tracer à la main f , S_1 , S_2 et S_3 sur un même graphique (repère orthonormé d'unité 8 cm par exemple), entre -1 et 1 .
2. Que peut-on observer ? Le signal f est-il continu ?
3. Intéressons-nous à la somme S_3 .
 - (a) Calculer sa dérivée.
 - (b) Montrer que S_3 est impaire et 1-périodique.
 - (c) Sur quel intervalle I simple suffit-il donc d'étudier S_3 ?
 - (d) Montrer que $\cos 6\pi t + \cos 10\pi t = 2 \cos 2\pi t \cos 8\pi t$.
 - (e) En déduire le tableau de variation de S_3 sur I .
4. Pour quelle abscisse t (comprise entre $\frac{1}{12}$ et $\frac{5}{12}$ strictement) la distance $|S_3(t) - f(t)|$ est-elle maximale ? Que vaut alors cette distance ?
5. Montrer, plus généralement, que $t = \frac{1}{4n}$ correspond au maximum de S_n sur $I = [0; 0,5[$, dans le cas où n est impair.

On pourra grouper les dérivées de S_n puis simplifier et montrer que $S'_n\left(\frac{1}{4n}\right) = 0$.

Que vaut ce maximum ?

On notera que cette hauteur constante est à l'origine du phénomène de Gibbs (c'est la crête persistante aux abords d'une discontinuité). Ce problème de convergence amène à la définition ultérieure des sommes de Fejér, qui sont des moyennes des sommes S_n destinées à « casser » cette crête.

DM 10. Le nombre e

10.1 Étude de deux suites

★

On pose, pour $n \geq 1$, $u_n = 1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!}$ et $v_n = u_n + \frac{1}{n \cdot n!}$.
On rappelle que $n! = 1 \times 2 \times \cdots \times n$.

1. Vérifier que $u_1 = 2$ et $v_1 = 3$. Calculer u_2 , u_3 , v_2 et v_3 .
2. Montrer que (u_n) est croissante et (v_n) décroissante.
3. Calculer $\lim_{n \rightarrow +\infty} \frac{1}{n \cdot n!}$. En déduire que les suites (u_n) et (v_n) sont adjacentes.
4. On note l leur limite commune. Déterminer un encadrement de l d'amplitude 10^{-3} .
Conjecturer la valeur exacte de l .

10.2 Calcul exact de la limite

★

★

Soit $n \geq 1$. On pose, pour $x \in [0; 1]$, $f(x) = \left(1 + \frac{x}{1!} + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!}\right) e^{-x}$

1. (a) Calculer $f(0)$ et vérifier que $f(1) = u_n \cdot e^{-1}$.
(b) Montrer que f est dérivable sur $[0; 1]$ et que $f'(x) = -\frac{x^n}{n!} e^{-x}$.
En déduire que $u_n \leq e$.
2. On pose, pour $x \in [0; 1]$, $g(x) = f(x) + \frac{x}{n!}$.
(a) Calculer $g'(x)$ et montrer que g est croissante sur $[0; 1]$.
(b) En déduire que $e - \frac{e}{n!} \leq u_n$.
3. Conclure sur la valeur exacte de l .

10.3 Irrationalité de e

★

★

Supposons que e est rationnel, i.e. qu'il existe deux entiers naturels tels que $e = \frac{p}{q}$.

1. Justifier $u_q < \frac{p}{q} < v_q$. En déduire que l'entier $N = p \cdot q! - q \cdot q! \cdot u_q$ vérifie $0 < N < 1$.
2. Le nombre e est-il rationnel?

Cette preuve fut donnée par Leonhard Euler, mathématicien suisse (1707-1783). Un siècle plus tard, Charles Hermite montra que e est transcendant, i.e. qu'il n'est racine d'aucun polynôme à coefficients entiers.

DM 11. Compléments sur l'exponentielle

11.1 Position par rapport aux tangentes

- ★
 1. Tracer \mathcal{C}_{\exp} et une tangente quelconque.
Quelle conjecture peut-on émettre sur leurs positions relatives?
 2. Montrer que \mathcal{C}_{\exp} est au-dessus de chacune de ses tangentes.
On prendra un réel donné, et on écrira l'équation de la tangente au point correspondant à cette abscisse.

11.2 Minorations polynômiales

- ★
 1. Montrer que $\exp(x) \geq 1 + x + \frac{x^2}{2}$ pour $x \geq 0$.
On pourra utiliser des calculs antérieurs...
 2. Montrer que $\exp(x) \geq 1 + x + \frac{x^2}{2} + \frac{x^3}{6}$ pour $x \geq 0$.
 3. Plus généralement, montrer par récurrence que $\exp(x) \geq 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots + \frac{x^n}{n!}$ pour $x \geq 0$.
 4. À partir de cette minoration, retrouver le résultat $\lim_{x \rightarrow +\infty} \frac{P(x)}{\exp(x)} = 0$ quel que soit le polynôme P .

11.3 Convexité

- ★
 1. Soient a et b deux réels, avec $a < b$. Soient $A(a; e^a)$ et $B(b; e^b)$. Soit t un réel, avec $0 \leq t \leq 1$.
 - ★
 1. Calculer les coordonnées du barycentre G_t de $\{(A, t), (B, 1 - t)\}$.
 2. Tracer \mathcal{C}_{\exp} puis prendre deux points A et B quelconques sur cette courbe.
Quelle semble être la position de la corde $[AB]$ par rapport à \mathcal{C}_{\exp} ?
Où peut se situer G_t ?
 3. Prouver que l'exponentielle est *convexe*, i.e. $\exp[ta + (1 - t)b] \leq t \exp(a) + (1 - t) \exp(b)$.
On pourra étudier la différence de ces deux expressions en fonction de t .
Traduire graphiquement ce résultat.
 4. En déduire que $\exp\left(\frac{a+b}{2}\right) \leq \frac{\exp(a) + \exp(b)}{2}$.

DM 12. Méthode de Newton

Soit f la fonction numérique définie sur \mathbb{R} par $f(x) = x \exp x - x - 1$ et soit \mathcal{C} sa courbe.

12.1 Étude générale et existence d'une racine

★

- (a) Calculer les limites de f au voisinage de $+\infty$ et de $-\infty$.
(b) Démontrer que la droite D d'équation $y = -x - 1$ est asymptote à \mathcal{C} .
- (a) Vérifier que f est dérivable, puis montrer que $f'(x) = x \exp x + \exp x - 1$.
(b) Étudier les signes de $\exp x - 1$ et de $x \exp x$.
(c) En déduire le sens de variation de f .
- (a) Montrer que l'équation $f(x) = 0$ admet exactement deux solutions sur \mathbb{R} .
(b) On note a la solution positive. Démontrer l'encadrement $0,8 \leq a \leq 0,81$.

12.2 Approximation de la racine

★
★
★

- Soit x_0 un réel strictement positif.
(a) On considère la tangente T à \mathcal{C} au point d'abscisse x_0 et on note x_1 l'abscisse du point de rencontre entre T et l'axe des abscisses. Montrer que $x_1 = x_0 - \frac{f(x_0)}{f'(x_0)}$.
(b) On considère la fonction φ définie sur \mathbb{R}_+^* par $\varphi(x) = x - \frac{f(x)}{f'(x)}$.
Vérifier l'existence de φ ainsi que l'égalité $\varphi(a) = a$.
On définit ainsi la suite d'approximation de a induite par la méthode de Newton. Il reste à contrôler l'erreur commise dans notre exemple.
- (a) Vérifier, sans calculer f'' , l'égalité $\varphi' = \frac{f f''}{f'^2}$.
(b) Calculer f'' .
(c) Montrer que f' et f'' sont croissantes sur \mathbb{R}_+^* .
(d) En déduire $0 \leq \varphi'(x) \leq \frac{f(0,81)f''(0,81)}{f'(0,8)^2} \leq 10^{-2}$ pour $a \leq x \leq 0,81$.
(e) En déduire, pour les mêmes valeurs de x , l'encadrement $0 \leq \varphi(x) - a \leq 10^{-2}(x - a)$.
(f) En déduire, pour les mêmes valeurs de x , l'encadrement $0 \leq \varphi(x) \leq 0,81$.
- On pose $x_0 = 0,81$ et $x_1 = \varphi(x_0)$.
(a) Montrer que $x_2 = \varphi(x_1)$ est une valeur approchée par excès de a à 10^{-6} près.
(b) Donner, à l'aide d'une calculatrice, une valeur approchée de x_2 .

DM 13. Complexes et polynômes

13.1 Racines carrées d'un complexe

- ★
1. Soit $Z = A + iB$ un complexe non nul.
Montrer qu'il existe deux complexes (opposés) z et $-z$ dont les carrés sont égaux à Z .
Aboutir à un système de deux équations réelles par identification, puis exploiter l'égalité des modules de z^2 et de Z .
 2. Déterminer les deux racines carrées de $e^{i\frac{\pi}{4}} = \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}$. En déduire $\cos \frac{\pi}{8}$ et $\sin \frac{\pi}{8}$.

13.2 Positions des racines d'un polynôme

- ★
★
- On pose $P(z) = z^4 - 6z^3 + 24z^2 - 18z + 63$.
1. Factoriser $P(z)$ dans \mathbb{C} .
On pourra remarquer que $i\sqrt{3}$ et $-i\sqrt{3}$ sont des racines.
 2. Montrer que les quatre points d'affixes les quatre racines trouvées appartiennent à un même cercle.

13.3 Racines d'un polynôme à coefficients réels

- ★
★
★
1. Soit $P(z) = a_n z^n + a_{n-1} z^{n-1} + \dots + a_1 z + a_0$ un polynôme complexe à coefficients réels.
Montrer que si z_0 est racine de P , alors $\overline{z_0}$ l'est également.
 2. Soit $Q(z) = (z - 1)(z - i)(z + 3)$. Le polynôme Q est-il à coefficients réels ?
 3. Montrer que $(z - z_0)(z - \overline{z_0})$ est un polynôme à coefficients réels.
 4. On admet pour l'instant que tout polynôme complexe possède au moins une racine (*théorème fondamental de l'algèbre*).
 - (a) Montrer qu'un polynôme complexe de degré n possède n racines (distinctes ou non).
 - (b) Montrer que tout polynôme réel se factorise en un produit de polynômes du premier degré ou du second degré avec un discriminant négatif.
 - (c) Soit $P(x) = x^4 + 1$. Vérifier que P ne possède pas de racine réelle mais se factorise pourtant dans \mathbb{R} .

13.4 Contrôle du module d'une racine d'un polynôme

- ★
★
★
- Soit z_0 une racine du polynôme $z^3 + pz + q$.
1. Si $|z_0| > 1$, établir que $|z_0|^3 \leq |pz_0| + |q| \leq |p||z_0| + |q||z_0|$.
 2. Montrer que $|z_0| \leq \max(1, |p| + |q|)$.

13.5 Théorème fondamental de l'algèbre



Soit $P \in \mathbb{C}[X]$ i.e. un polynôme complexe à coefficients complexes (et donc éventuellement réels). Nous allons prouver que si P n'est pas constant, alors il possède au moins une racine complexe.

Ce théorème fut presque prouvé par d'Alembert, mais réellement démontré plus tard par Gauss. En France, il est connu sous le nom de théorème de D'Alembert-Gauss, les autres nations ayant surtout retenu Gauss...

Complément : $z \rightarrow a$ si $|z - a| \rightarrow 0$ et $z \rightarrow \infty$ si $|z| \rightarrow \infty$.

1. Montrer que $\lim_{z \rightarrow \infty} |P(z)| = +\infty$.
2. Raisonnons par l'absurde, et supposons que P ne s'annule jamais.
Montrer l'idée, en considérant $\frac{1}{|P(z)|}$, qui prouve que $|P(z)|$ possède (au moins) un minimum m en un point z_0 de \mathbb{C} .
On veut donc montrer que m est nul.
3. Soit Q le polynôme défini par $Q(z) = \frac{P(z + z_0)}{P(z_0)}$.
Montrer que $|Q(z)|$ est minimal lorsque $z = 0$ puis que $Q(0) = 1$.
4. Soit $p \geq 1$ la plus petite puissance de z dans $Q(z) = \sum_k a_k z^k$.
Montrer que $Q(z) = 1 + a_p z^p (1 + \mu(z))$ où $\lim_{z \rightarrow 0} \mu(z) = 0$.
5. On pose $\rho = |a_p|$ et $z = r e^{it}$.
Montrer qu'on peut trouver t afin que $a_p e^{ipt} = -\rho$.
6. Montrer que $Q(z) = 1 - \rho r^p (1 + \varepsilon(z) + i\eta(z))$ où ε et η sont des fonctions à valeurs réelles tendant vers 0 en $z = 0$.
7. Montrer, par un calcul direct, que $|Q(z)|^2 = 1 - 2\rho r^p + r^p \xi(r)$ où ξ tend vers 0 en 0.
8. Montrer que si r est assez petit, $|Q(z)|^2 < 1$.
9. Constater que ceci contredit la valeur du minimum de $|Q(z)|$.

Il est remarquable qu'il n'existe aucune preuve du théorème fondamental de l'algèbre évitant un recours à un argument analytique.

DM 14. Complexes et électronique linéaire

14.1 Impédance

- ★
★
1. Considérons une grandeur sinusoïdale dépendant du temps, $x(t) = A \sin(\omega t + \varphi)$. Nommer les constantes A, ω, φ . Sous GeoGebra, créer 3 curseurs nommés A, ω et φ , avec des plages pertinentes, puis tracer la fonction $x(t)$. Jouer ensuite sur les curseurs et décrire les changements opérés sur la courbe.

Il est commode de définir la fonction complexe

$$\underline{X}(t) = Ae^{j(\omega t + \varphi)} = Ae^{j\varphi} e^{j\omega t}$$

en rappelant qu'ici $j^2 = -1$, notation standard en électronique.

On appelle $Ae^{j\varphi}$ l'*amplitude complexe* de $x(t)$.

2. Considérons maintenant un dipôle *linéaire* traversé par un courant sinusoïdal

$$i(t) = I \sin(\omega t + \varphi).$$

On a alors

$$u(t) = U \sin(\omega t + \psi)$$

ce qui signifie que u est sinusoïdal et possède la *même* fréquence que i .

Soient \underline{I} et \underline{U} les fonctions complexes associées à i et u .

Montrer que l'*impédance* complexe du dipôle, définie par

$$\underline{Z} = \frac{\underline{U}}{\underline{I}}$$

vaut $Ze^{j(\psi - \varphi)}$ où $Z = \frac{U}{I}$. On a ainsi

$$\underline{U} = \underline{Z} \times \underline{I}.$$

Si l'on écrit la forme algébrique $\underline{Z} = R + jX$, alors $R = \text{Re}(\underline{Z})$ est la *résistance* et $X = \text{Im}(\underline{Z})$ la *réactance*.

14.2 Propriétés

★
★

1. Si des dipôles D_k sont montés en *série*, montrer que les impédances s'ajoutent : $\underline{Z} = \sum_k \underline{Z}_k$.

Si les dipôles sont montés en *parallèle*, montrer que $\frac{1}{\underline{Z}} = \sum_k \frac{1}{\underline{Z}_k}$.

La quantité $\underline{Y} = \frac{1}{\underline{Z}}$ est l'*admittance* du circuit.

Ainsi, en parallèle, les admittances s'ajoutent.

2. On rappelle que

- pour une *résistance* R , on a $u = Ri$;
- pour une *inductance* L , on a $u = L \frac{di}{dt}$;
- pour une *capacité* C , on a $i = C \frac{du}{dt}$.

(a) Déterminer l'impédance de chacun de ces dipôles.

(b) En déduire l'impédance d'un circuit RLC parallèle.

(c) Déterminer la pulsation *critique* ω_0 telle que cette impédance soit réelle.

(d) Finalement, montrer que l'impédance du circuit vaut :

$$\underline{Z} = \frac{R}{1 + jQ \left(\frac{\omega}{\omega_0} - \frac{\omega_0}{\omega} \right)}$$

où $Q = RC\omega_0$ est le *coefficient de qualité*.

14.3 Représentation de l'impédance

★
★
★

1. Montrer alors que

$$\begin{cases} |\underline{Z}| = \frac{R}{\sqrt{1 + Q^2 \left(\frac{\omega}{\omega_0} - \frac{\omega_0}{\omega} \right)^2}} \\ \arg \underline{Z} = -\arctan \left[Q \left(\frac{\omega}{\omega_0} - \frac{\omega_0}{\omega} \right) \right] \end{cases}$$

2. On prend ici $R = 100\Omega$, $L = 0,1mH$ et $C = 10\mu F$.

Tracer, dans le plan complexe, la courbe décrite par le point $M(\underline{Z})$ lorsque ω varie entre 0 et $+\infty$. Cette courbe est le *diagramme de Nyquist* du circuit RLC parallèle. Quelle figure géométrique obtient-on sous GeoGebra ?

3. Quel lieu géométrique décrit le point d'affixe $1 + jQ \left(\frac{\omega}{\omega_0} - \frac{\omega_0}{\omega} \right)$ lorsque ω parcourt \mathbb{R}_+ ?

Quelle est l'image de la droite d'équation $x = 1$ par l'application complexe $z \mapsto \frac{1}{z}$?

Montrer alors que la forme du diagramme est un cercle à préciser.

DM 15. Complexes et géométrie

15.1 Homographie et cercles

★

Le plan est rapporté à un repère orthonormé direct (O, \vec{u}, \vec{v}) . On appelle f l'application qui, à tout point M d'affixe $z \neq -1$, associe le point M' d'affixe $z' = \frac{-iz - 2}{z + 1}$. Soient A , B et C les points d'affixes respectives $a = -1$, $b = 2i$ et $c = -i$.

1. Soit C' l'image de C par f .

Déterminer l'affixe c' du point C' sous forme algébrique, puis sous forme trigonométrique.

2. Calculer l'affixe d du point D ayant pour image le point D' d'affixe $d' = \frac{1}{2}$.
3. Pour tout nombre complexe $z \neq -1$, on note p le module de $z + 1$ et p' le module de $z' + i$.
 - (a) Démontrer que, pour tout nombre complexe $z \neq -1$, on a $pp' = \sqrt{5}$.
 - (b) Si le point M appartient au cercle Γ de centre A et de rayon 2, montrer qu'alors $M' = f(M)$ appartient à un cercle Γ' dont on précisera le centre et le rayon.
4. Pour tout nombre complexe $z \neq -1$, on considère le nombre complexe $\omega = \frac{z - 2i}{z + 1}$.
 - (a) Interpréter géométriquement l'argument de ω .
 - (b) Montrer que $z' = -i\omega$.
 - (c) Déterminer l'ensemble F des points M d'affixe z telle que z' soit un réel non nul.
 - (d) Vérifier que D appartient aux ensembles Γ et F .
5. Représenter grâce à GeoGebra les ensembles Γ , F et Γ' .

15.2 Suites de Mendès-France

★

★

★

Les *suites de Mendès-France* sont de la forme $z_{n+1} = z_n + e^{i2\pi f(n)}$ où f est une fonction. Elles sont utiles dans l'étude de l'équirépartition de la partie décimale de la suite $f(n)$.

On utilisera un tableur ou un logiciel de programmation, en traçant via les parties réelle et imaginaire beaucoup de points $M_n(z_n)$.

1. Quelle est la distance séparant z_n et z_{n+1} ?
2. Que représente géométriquement le nombre $2\pi f(n)$?
3. Pourquoi la partie entière de $f(n)$ n'est d'aucune importance ?
4. Représenter (M_n) pour $f(n) = n\sqrt{2}$, $f(n) = n^{1,2}$ et $f(n) = n^{1,9}$.

DM 16. Applications du logarithme

16.1 Sismologie



La *magnitude* d'un séisme d'intensité I est mesurée sur l'*échelle de Richter* par $M = \log \frac{I}{I_0}$, où I_0 est une intensité de référence.

1. Calculer la magnitude des séismes suivants :
 - (a) Îles Macquaries 1989 : $I = 1,995 \cdot 10^8 \cdot I_0$;
 - (b) Californie 1992 : $I = 3,16 \cdot 10^7 \cdot I_0$;
 - (c) Indonésie 1993 : $I = 6,3 \cdot 10^6 \cdot I_0$.
2. Dans nos régions, un fort séisme est de magnitude 4,8 ; le séisme de 2006 ayant causé un tsunami a atteint la magnitude 7,9. Comparer les intensités de ces deux séismes.
3. Quel facteur d'intensité séparent deux séismes de différence de magnitude égale à 1 ?
4. L'énergie E (en joules) libérée au foyer du séisme est liée à la magnitude par la relation $\log E = a + bM$ où a et b sont des constantes. Calculer a et b sachant qu'un séisme de magnitude 8 met en jeu environ 30.000 fois plus d'énergie qu'un séisme de magnitude 5, lui-même délivrant une énergie de $0,2 \cdot 10^{20}$ joules.

16.2 Radioactivité



La loi d'évolution du nombre de noyaux d'un corps radioactif est donnée par $N_t = N_0 e^{-at}$, où a est une constante positive.

1. Représenter graphiquement l'allure de la fonction $t \mapsto N_t$.
2. On désigne par T le temps (*demi-vie*) au bout duquel $N_T = \frac{1}{2} N_0$.
Exprimer a en fonction de T . Comparer N_{t+T} à N_t .
3. Au bout de combien de temps un corps composé de 1 g de radium perdra-t-il une masse de 1 mg, sachant que la demi-vie du radium est de 1622 ans et que la masse est proportionnelle au nombre d'atomes ?

16.3 Astronomie

★
★ La *magnitude apparente* d'un astre d'éclat E est définie à partir d'un éclat de référence E_0 par $M = \log_a \left(\frac{E}{E_0} \right)$. La convention est que la magnitude augmente de 5 lorsque l'éclat est divisé par 100.

1. Calculer $\log a$.
2. Déterminer la magnitude apparente des astres suivants :
 - (a) Soleil : $E = 4,786 \cdot 10^{10} \cdot E_0$;
 - (b) Lune : $E = 1,2 \cdot 10^5 \cdot E_0$.

16.4 Acoustique

★ Le niveau sonore en *décibels* (dB) d'un son de pression acoustique P est donné par la relation $L = 10 \log \frac{P}{P_0}$, où $P_0 = 2 \cdot 10^{-5}$ Pa est la plus petite pression perceptible par une oreille humaine.

1. Calculer les niveaux sonores correspondant :
 - (a) au seuil d'audibilité ($P = P_0$) ;
 - (b) à une conversation courante ($P = 10^3 P_0$) ;
 - (c) à une fusée au décollage ($P = 10^9 P_0$).
2. Un baladeur, à la puissance maximale, peut atteindre 105 dB. Calculer le rapport $\frac{P}{P_0}$.
3. Quelle augmentation en décibels correspond à un doublement de la puissance sonore ?

16.5 Datation

★ Les archéologues et les paléontologues datent les objets découverts contenant du carbone en mesurant la proportion de l'un de ses isotopes, le *carbone 14*, encore présent dans l'objet. À la mort d'un être vivant, le carbone 14 présent dans son organisme se désintègre au fil des ans, de sorte que, si p est la proportion de C_{14} restante au bout de N années, alors $N = -8310 \ln p$.

1. Le squelette d'un homme de Cro-Magnon contient 5% du carbone initial. Quel est son âge ?
2. Lucy est un des plus anciens hominidés connu ; les spécialistes lui donnent 3,2 millions d'années. A-t-on pu raisonnablement dater ses fragments à l'aide du carbone 14 ?
3. Hibernatus, découvert dans un glacier en 1991, contenait 52,8% (à 1% près) du carbone initial. Donner un encadrement de son âge.

DM 17. Compléments sur le logarithme

17.1 Développement limité

★

★

1. Étudier le sens de variation de $f : x \mapsto x - \frac{x^2}{2} + \frac{x^3}{3} - \ln(1+x)$ sur $] -1; +\infty[$.
En déduire le signe de $f(x)$ sur cet intervalle.
2. De même, étudier le signe de $g(x) = \ln(1+x) - \left(x - \frac{x^2}{2}\right)$ sur $[0; +\infty[$.
3. De même, étudier le signe de $h(x) = \ln(1+x) - \left(x - \frac{x^2}{2} + \frac{2x^3}{3}\right)$ sur $\left[-\frac{1}{2}; 0\right]$.
4. En déduire les encadrements :
 - (a) $x - \frac{x^2}{2} \leq \ln(1+x) \leq x - \frac{x^2}{2} + \frac{x^3}{3}$ pour $x \geq 0$;
 - (b) $x - \frac{x^2}{2} + \frac{2x^3}{3} \leq \ln(1+x) \leq x - \frac{x^2}{2} + \frac{x^3}{3}$ pour $-\frac{1}{2} \leq x \leq 0$.
5. *Application.* Étudier la limite éventuelle en 0 de $\frac{\ln(1+x) - x}{x^2}$.

17.2 Constante d'Euler

★

★

★

1. On considère la suite (u_n) définie pour $n \geq 1$ par $u_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$.
 - (a) Calculer de manière approchée quelques termes de cette suite, grâce à un tableur.
 - (b) Pour $x \geq 0$, démontrer les inégalités $\ln(1+x) \leq x$ et $\frac{x}{1+x} \leq \ln(1+x)$.
En déduire que, pour $k \geq 1$, $\frac{1}{k+1} \leq \ln(k+1) - \ln k \leq \frac{1}{k}$.
 - (c) En effectuant une sommation sur l'encadrement précédent, prouver que pour tout $n \geq 1$, $u_{n+1} - 1 \leq \ln(n+1) \leq u_n$. En déduire que $\ln(n+1) \leq u_n \leq 1 + \ln n$.
 - (d) Quelle est la limite de (u_n) ?
 - (e) Déterminer un entier n_0 pour lequel u_{n_0} dépasse 100.
2. On considère la suite (c_n) définie pour $n \geq 2$ par $c_n = u_{n-1} - \ln n$.
 - (a) Calculer $c_{n+1} - c_n$. En déduire le sens de variation de (c_n) .
 - (b) Montrer que, pour tout $n \geq 2$, $c_n \leq 1 + \ln(n-1) - \ln n$.
 - (c) En déduire que (c_n) est majorée et convergente.
On note γ sa limite, appelée *constante d'Euler*.
3. Calculer c_{10000} , i.e. une valeur approchée de γ .

DM 18. Conditionnement et indépendance

18.1 Surprises conditionnelles

★

1. David a deux enfants dont au moins une fille.
Quelle est la probabilité que l'autre soit un garçon ?
2. Claire a deux enfants. Le plus jeune est une fille.
Quelle est la probabilité que l'aîné soit un garçon ?
3. Quel sentiment émerge de ces deux réponses ? Sont-elles surprenantes ?

18.2 Indépendances

★

★

Trois événements A , B et C sont *globalement indépendants* si $P(A \cap B \cap C) = P(A)P(B)P(C)$.
On jette deux dés, un noir et un blanc. Soient $A =$ « le chiffre du dé noir est pair », $B =$ « le chiffre du dé blanc est impair » et $C =$ « les deux chiffres ont même parité ».
Montrer que ces événements sont deux à deux indépendants, mais cependant pas globalement indépendants.

18.3 Transmission d'une rumeur

★

★

★

On considère n individus I_1, I_2, \dots, I_n . L'individu I_1 reçoit une rumeur sous la forme de « oui » ou de « non », puis la transmet à I_2 et ainsi de suite jusqu'à I_n . Le dernier individu I_n rend publique la rumeur. Chaque individu transmet correctement ce qu'il a entendu avec une même probabilité p , où $0 < p < 1$. On suppose les n individus indépendants, même s'ils se connaissent.

On pose $\Omega = \{(\omega_1, \dots, \omega_n), \omega_i = \pm 1\}$ où $\omega_i = +1$ si la i -ième personne transmet fidèlement l'information et $\omega_i = -1$ sinon. Soit P la probabilité pertinente pour notre problème.

1. Montrer que $P(\{(\omega_1, \dots, \omega_n)\}) = k_1 \cdots k_n$ où $k_i = p$ si $\omega_i = +1$ et $k_i = 1 - p$ sinon.
2. Posons $A_i =$ « I_i transmet l'information initiale » et $B_i =$ « I_i transmet ce qu'il a entendu ».
Montrer que $A_i = (A_{i-1} \cap B_i) \cup (\overline{A_{i-1}} \cap \overline{B_i})$.
En déduire que $P(A_i) = P(A_{i-1} \cap B_i) + P(\overline{A_{i-1}} \cap \overline{B_i})$.
3. Posons $p_i = P(A_i)$. Montrer que $p_i = 1 - p + (2p - 1)p_{i-1}$ si $i \geq 2$ (et $p_1 = p$).
4. Quelle est la seule limite ℓ possible de la suite (p_i) ?
Montrer que $(p_i - \ell)$ est géométrique ; en déduire son terme général, puis celui de (p_i) .
Que vaut la limite de (p_i) ?
5. Conclure sur ce qu'on vient concrètement de montrer.

DM 19. Probabilités en biologie

19.1 Formule de Bayes

★ Soit M une maladie. On suppose que M affecte un Français sur 1000. On dispose d'un test sanguin, qui détecte M avec une fiabilité de 99% lorsque cette maladie est effectivement présente. Cependant, on obtient un résultat faussement positif pour 0,2% des personnes saines testées.

1. Construire l'arbre de ce problème.
2. Soit E l'ensemble des personnes atteintes de M .
Soit T l'ensemble des personnes ayant une réaction positive au test.
(a) Montrer la *formule de Bayes* :

$$P_T(E) = \frac{P(E)P_E(T)}{P(E)P_E(T) + P(\overline{E})P_{\overline{E}}(T)}.$$

- (b) En déduire $P_T(E)$.
3. Que peut-on en penser concrètement ?
Que permet de faire la formule de Bayes (parfois appelée probabilité des causes...) ?

19.2 Théorème d'Hardy-Weinberg

★
★ On considère une population (génération 0), dans laquelle les proportions de génotypes AA , Aa et aa sont p_0 , q_0 et r_0 respectivement. On admet que les couples se forment au hasard quant aux génotypes considérés (i.e. l'appariement est aléatoire).

1. Calculer $p_0 + q_0 + r_0$.
2. Exprimer, en fonction de p_0 , q_0 et r_0 , les probabilités p_1 , q_1 et r_1 qu'un enfant de la génération 1 ait les génotypes AA , Aa et aa respectivement.
On pourra faire un arbre.
3. Montrer que $p_1 = \left(\frac{\alpha + 1}{2}\right)^2$, $q_1 = \frac{1 - \alpha^2}{2}$ et $r_1 = \left(\frac{1 - \alpha}{2}\right)^2$, où $\alpha = p_0 - r_0$.
4. Comparer $p_1 - r_1$ et $p_0 - r_0$.
5. En déduire p_2 , q_2 et r_2 , puis p_n , q_n et r_n .
6. Que dire des suites (p_n) , (q_n) et (r_n) ?
7. Interpréter concrètement ce résultat (*loi d'Hardy-Weinberg*).

DM 20. Intégration et ordre

20.1 Suites et intégrales

★

1. Soit f une fonction continue sur $[0; 1]$ telle que, pour tout x de $[0; 1]$, $m \leq f(x) \leq M$. Déterminer la limite de la suite de terme général $u_n = \int_0^{\frac{1}{n}} f(x) \, dx$.
2. (a) Soit f une fonction continue, monotone sur \mathbb{R}_+ et vérifiant $\lim_{t \rightarrow +\infty} f(t) = a$ où a est un réel donné. On pose $I_n = \int_n^{n+1} f(t) \, dt$. Montrer que $\lim_{n \rightarrow +\infty} I_n = a$.
(b) *Application.* Étudier les limites des suites de termes généraux :
 $I_n = \int_n^{n+1} \frac{dt}{1+t^2}$; $I_n = \int_n^{n+1} \frac{t}{1+t^2} \, dt$; $I_n = \int_n^{n+1} \ln \left(\frac{5t+1}{t+3} \right) dt$.

20.2 Intégration des fonctions périodiques

★

★

- Soit f une fonction continue sur \mathbb{R} et T -périodique.
1. Soit F une primitive de f . Soit $G(t) = F(t+T) - F(t)$, pour $t \in \mathbb{R}$. Montrer que G est constante sur \mathbb{R} .
 2. L'intégrale $\int_a^{a+T} f(t) \, dt$ dépend-elle du nombre réel a choisi ?
Ainsi, la somme d'une fonction périodique est la même sur n'importe quelle période.
 3. *Application.* Montrer sans calcul que $\int_0^{2\pi} \sin t \, dt$ est nulle.

20.3 Inégalité de Cauchy-Schwarz

★

★

★

- Soient f et g deux fonctions continues sur un intervalle contenant a et b .
Soit $P(\lambda) = \int_a^b [\lambda f(t) + g(t)]^2 \, dt$ où $\lambda \in \mathbb{R}$.
1. Vérifier que P est bien définie.
 2. Montrer que $P(\lambda)$ est un trinôme de second degré au maximum.
On montrera que $P(\lambda) = A\lambda^2 + B\lambda + C$, où A, B, C sont à déterminer.
 3. Que signifie le cas $A = 0$ pour la fonction f ?
 4. On suppose maintenant $A > 0$. Montrer que $P(\lambda) \geq 0$.
En déduire que $B^2 \leq 4AC$.
 5. Établir alors l'inégalité de Cauchy-Schwarz : $\left(\int_a^b fg \right)^2 \leq \left(\int_a^b f^2 \right) \left(\int_a^b g^2 \right)$.

DM 21. Intégration et sommes

21.1 Centre d'inertie d'un demi-disque

★
★
★

Considérons A le demi-disque (supérieur) de centre O et de rayon 1 (plaque homogène). Soit, pour k allant de 0 à $n - 1$, le rectangle horizontal R_k défini par

- son centre est le point O_k de coordonnées $(0; y_k)$;
- $y_k = \frac{1}{2} \frac{1}{n} + k \frac{1}{n}$;
- sa hauteur est $\frac{1}{n}$;
- sa largeur est celle du disque à l'ordonnée y_k .

1. Dessiner A et les rectangles R_k pour $n = 8$.
2. Déterminer simplement les coordonnées du centre d'inertie d'un rectangle R_k .
3. Calculer l'aire de R_k en fonction de n et de y_k .
4. Soit A_n la plaque formée des n rectangles R_k . Montrer que les coordonnées du centre d'inertie de A_n sont $x = 0$ et

$$y = \frac{1}{\text{aire}(A_n)} \sum_{k=0}^{n-1} \frac{1}{n} y_k 2\sqrt{1 - y_k^2}.$$

5. On sait que l'aire de A_n tend vers celle de A lorsque n tend vers $+\infty$. Justifier par la méthode des rectangles que l'ordonnée du centre d'inertie de A est $\frac{1}{\pi/2} \int_0^1 2y\sqrt{1 - y^2} dy$.
6. Calculer cette intégrale par simple primitivation, et montrer que sa valeur est $\frac{4}{3\pi}$.
7. Conclure sur la position du centre d'inertie d'un demi-disque quelconque.
8. Essayer de trouver un moyen de se souvenir de l'intégrale de la question 5, y compris grâce au dy , en pensant au langage habituel de la physique.

21.2 Encadrement du logarithme népérien

★
★

1. Montrer que, pour $x \geq 0$, on a $1 - x \leq \frac{1}{1+x} \leq 1 - x + x^2$.
2. En déduire que, pour $x \geq 0$, on a $x - \frac{x^2}{2} \leq \ln(1+x) \leq x - \frac{x^2}{2} + \frac{x^3}{3}$.

21.3 Approximation de π par la méthode de l'arctangente

★
★
★

Soit, pour $n \geq 1$,

$$u_n = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots + \frac{(-1)^n}{2n+1}.$$

1. Montrer que, pour tout réel t ,

$$\left(1 - t^2 + t^4 + \cdots + (-1)^n t^{2n}\right) - \frac{1}{1+t^2} = (-1)^n \frac{t^{2n+2}}{1+t^2}.$$

On pourra se souvenir de la somme des termes d'une suite géométrique...

2. En déduire que

$$u_n - \int_0^1 \frac{dt}{1+t^2} = (-1)^n \int_0^1 \frac{t^{2n+2}}{1+t^2} dt.$$

3. Montrer que, pour tout réel $t \in [0; 1]$, $\frac{t^{2n+2}}{1+t^2} \leq t^{2n+2}$.

4. En déduire que

$$\left| u_n - \int_0^1 \frac{dt}{1+t^2} \right| \leq \frac{1}{2n+3}.$$

5. Quelle est la valeur de

$$\int_0^1 \frac{dt}{1+t^2} ?$$

On pourra se souvenir d'un devoir sur l'arctangente...

6. En déduire que (u_n) converge vers $\frac{\pi}{4}$.
7. Déterminer un entier n_0 tel que $4u_{n_0}$ soit une valeur approchée de π à 10^{-2} près.
8. Représenter l'évolution de la suite, pour $n = 10, 20, \dots, 100$.
9. La convergence semble-t-elle rapide ?

DM 22. Intégrales trigonométriques

22.1 Intégrale de Wallis



Soit $n \in \mathbb{N}$. On pose

$$I_n = \int_0^{\frac{\pi}{2}} (\sin x)^n dx.$$

1. Calculer I_0 et I_1 .

2. Montrer que, pour $n \geq 2$, on a $I_n = \frac{n-1}{n} I_{n-2}$.

On pourra faire une intégration par parties en écrivant $(\sin x)^n = (\sin x)^{n-1} \sin x$.

3. En déduire I_2, \dots, I_5 .

4. Démontrer par récurrence que, pour $n \geq 1$,

$$\begin{cases} I_{2n} = \frac{1 \times 3 \times 5 \times \dots \times (2n-1)}{2 \times 4 \times 6 \times \dots \times (2n)} \times \frac{\pi}{2} \\ I_{2n+1} = \frac{2 \times 4 \times 6 \times \dots \times (2n)}{1 \times 3 \times 5 \times \dots \times (2n-1)} \times \frac{1}{2n+1} \end{cases}$$

5. Pour $x \in \left[0; \frac{\pi}{2}\right]$, comparer $(\sin x)^n$ et $(\sin x)^{n+1}$.

En déduire que la suite (I_n) est décroissante.

6. En utilisant la question 2, établir pour $n \geq 1$ l'encadrement $\frac{n}{n+1} I_{n-1} \leq I_n \leq I_{n-1}$.

7. En déduire que $\lim_{n \rightarrow +\infty} \frac{I_{2n+1}}{I_{2n}} = 1$.

8. Montrer la *formule de Wallis* :

$$\lim_{n \rightarrow +\infty} w_n = \frac{\pi}{2}$$

où, pour $n \geq 1$,

$$w_n = \left(\frac{2 \times 4 \times 6 \times \dots \times (2n)}{1 \times 3 \times 5 \times \dots \times (2n-1)} \right)^2 \times \frac{1}{2n+1}.$$

22.2 Somme des inverses des carrés

★
★
★

On veut ici étudier la limite de la suite de terme général $u_n = \frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{n^2}$.

1. (a) Calculer $J = \int_0^\pi \left(\frac{t^2}{2\pi} - t \right) dt$.
 - (b) On pose, pour $k \geq 1$, $K = \int_0^\pi \left(\frac{t^2}{2\pi} - t \right) \cos kt \, dt$. Montrer que $K = \frac{1}{k^2}$ grâce à deux intégrations par parties.
 - (c) On appelle *noyau de Dirichlet* la fonction définie pour tout $t \in [0; \pi]$ et $n \geq 1$ par $D_n(t) = \frac{1}{2} + \cos t + \cos 2t + \cdots + \cos nt$. Montrer que $u_n = \frac{\pi^2}{6} + \int_0^\pi \left(\frac{t^2}{2\pi} - t \right) D_n(t) \, dt$.
On note I_n cette dernière intégrale.
2. (a) i. Vérifier que $2 \sin b \cos a = \sin(a + b) - \sin(a - b)$.
 - ii. En déduire par récurrence que, pour tout $t \in]0; \pi]$ et $n \geq 1$, $D_n(t) = \frac{\sin \left(n + \frac{1}{2} \right) t}{2 \sin \frac{t}{2}}$.
 - iii. Soit g la fonction définie sur $[0; \pi]$ par $g(0) = -1$ et $g(t) = \frac{\frac{t^2}{2\pi} - t}{2 \sin \frac{t}{2}}$ si $t \neq 0$.
Montrer que g est continue en 0.
 - iv. Montrer que, pour $n \geq 1$, $I_n = \int_0^\pi g(t) \sin \left(n + \frac{1}{2} \right) t \, dt$.
- (b) i. Montrer que g est dérivable sur $]0; \pi]$, puis calculer g' .
 - ii. Montrer que g est dérivable en 0 et calculer $g'(0)$.
 - iii. Montrer que g' est continue en 0.
 - iv. En déduire que g' est continue sur $[0; \pi]$.
3. (a) Montrer que $I_n = \frac{-1}{n + \frac{1}{2}} + B_n$, où $B_n = \int_0^\pi g'(t) \frac{\cos(n + \frac{1}{2})t}{n + \frac{1}{2}} dt$.
On justifiera bien les hypothèses nécessaires à cette IPP.
 - (b) Pourquoi g' est-elle bornée sur $[0; \pi]$?
 - (c) En déduire que $\lim_{n \rightarrow +\infty} B_n = 0$ puis que $\lim_{n \rightarrow +\infty} I_n = 0$.
4. Que vaut la limite de (u_n) ? La convergence semble-t-elle rapide ?

DM 23. Produit scalaire dans l'espace

23.1 Orthogonalité de deux droites



On considère un cube $ABCDEFGH$ de côté 1, avec E au-dessus de A . Soient :

- I et J les milieux des arêtes $[GH]$ et $[BF]$;
- P et Q les points d'intersection d'une part de (EG) et (FI) , et d'autre part de (FC) et (GJ) .

On veut prouver de différentes manières que la droite (PQ) est orthogonale aux droites (EG) et (FC) .

1. Montrer que P et Q sont les centres d'inertie respectifs des triangles FGH et FBG .
2. *Coordonnées.* Introduire un repère orthonormal adapté au problème, puis calculer les coordonnées de \overrightarrow{EG} , \overrightarrow{FC} , P , Q , \overrightarrow{PQ} . Calculer $\overrightarrow{PQ} \cdot \overrightarrow{EG}$ et $\overrightarrow{PQ} \cdot \overrightarrow{FC}$. Conclure.
3. *Produit scalaire.* Montrer que $3\overrightarrow{PQ} = \overrightarrow{GB} + \overrightarrow{GF} - \overrightarrow{GE}$. En déduire $\overrightarrow{PQ} \cdot \overrightarrow{EG} = 0 = \overrightarrow{PQ} \cdot \overrightarrow{FC}$. Conclure.
4. *Transformation.* On rappelle que la grande diagonale du cube (BH) est orthogonale au plan (ACF) . Soit K le milieu de $[FG]$. Quelles sont les images de H et de B par l'homothétie de centre K et de rapport $\frac{1}{3}$? Conclure.

23.2 Propriétés du tétraèdre régulier



Soit $ABCD$ un tétraèdre régulier d'arête a .

1. Soit H le projeté orthogonal de A sur (BCD) .
 - (a) Montrer que H est équidistant des trois sommets B , C et D .
En déduire que $\overrightarrow{AB} + \overrightarrow{AC} + \overrightarrow{AD} = 3\overrightarrow{AH}$
 - (b) Calculer en fonction de a le carré scalaire $(\overrightarrow{AB} + \overrightarrow{AC} + \overrightarrow{AD})^2$. En déduire AH .
 - (c) Soient E et F les milieux respectifs de $[AD]$ et $[BC]$. Montrer que $2\overrightarrow{EF} = \overrightarrow{AB} + \overrightarrow{DC}$.
En déduire EF .
2. Montrer que $\overrightarrow{AB} \cdot \overrightarrow{AC} = \overrightarrow{AC} \cdot \overrightarrow{AD} = \overrightarrow{AD} \cdot \overrightarrow{AB} = \frac{a^2}{2}$. Que peut-on en déduire sur les positions relatives des droites (AB) et (CD) ?

DM 24. Systèmes linéaires

24.1 Calculs d'entraînement

★
★

1. Résoudre chaque système par la méthode du pivot de Gauss :

(a)

$$\begin{cases} x + y + z = 1 \\ x - y + z = 2 \\ x - y - z = 3 \end{cases} \quad \begin{cases} x - y + 4z = 1 \\ 2x + y - z = 1 \\ -x - y + 2z = 1 \end{cases}$$

(b)

$$\begin{cases} x + 2y - 6z = 4 \\ 2x - 2y + 3z = 4 \\ x + 8y - 21z = 6 \end{cases} \quad \begin{cases} x + 3y + z = 0 \\ x + y - z = 0 \\ x - 2y - 4z = 0 \end{cases}$$

2. Résoudre chaque système par une méthode quelconque :

$$\begin{cases} 5x + 2z = 1 \\ y - 3z = 2 \\ 2x + y = 3 \end{cases} \quad \begin{cases} x + y - 2z = 1 \\ y + z = 1 \\ x - y - 4z = 1 \end{cases}$$

24.2 Nouvelle base de l'espace des polynômes $\mathbb{R}[x]$

★
★
★

1. (a) Déterminer trois réels a , b et c tels que

$$x^2 = a(x-1)^2 + b(x-1) + c$$

pour tout x réel.

(b) En déduire une primitive sur \mathbb{R} de la fonction f définie par $f(x) = x^2(x-1)^{666}$.

2. On peut se poser la question de l'existence et de l'unicité de l'écriture de n'importe quel polynôme avec des monômes du type $(x-1)^n$.

- (a) i. Par récurrence sur le degré, montrer que tout monôme x^n est un polynôme de la variable $(x-1)$.

On pourra remarquer que $x^n = (x-1)x^{n-1} + x^{n-1} \dots$

- ii. En déduire que tout polynôme de la variable x est aussi un polynôme de la variable $(x-1)$.

- (b) i. Soit $P(x) = a_n(x-1)^n + a_{n-1}(x-1)^{n-1} + \dots + a_1(x-1) + a_0$.

Si $P(x) = 0$ quel que soit x , que peut-on affirmer sur ses coefficients a_k ?

- ii. Les coefficients d'un polynôme écrit avec la variable $(x-1)$ sont-ils uniques ?

On a ainsi prouvé que l'ensemble $\{(x-1)^n, n \in \mathbb{N}\}$ forme une base de l'espace vectoriel des polynômes réels : tout polynôme réel peut s'écrire comme une combinaison linéaire d'éléments de cette base, cette décomposition étant unique.

DM 25. Géométrie analytique

25.1 Premier QCM



On munit l'espace d'un repère orthonormal.
 \mathcal{D} est la droite d'équation paramétrique :

$$\begin{cases} x = 1 + 2t \\ y = 2 - t \\ z = -3 - t \end{cases}.$$

\mathcal{P} est le plan d'équation cartésienne $x + 2y - 3z - 1 = 0$. Donner la réponse exacte parmi les trois affirmations proposées :

1. (a) Le point $M(-1; 3; 2)$ appartient à \mathcal{D} ;
(b) le point $N(2; -1; -1)$ appartient à \mathcal{D} ;
(c) le point $R(3; 1; -4)$ appartient à \mathcal{D} .
2. (a) Le vecteur $\vec{u}(1; 2; -3)$ dirige \mathcal{D} ;
(b) le vecteur $\vec{v}(-2; 1; 1)$ dirige \mathcal{D} ;
(c) le vecteur $\vec{w}(3; 1; -4)$ dirige \mathcal{D} .
3. (a) \mathcal{D} est incluse dans \mathcal{P} ;
(b) \mathcal{D} est strictement parallèle à \mathcal{P} ;
(c) \mathcal{D} est sécante avec \mathcal{P} .
4. (a) $G(1; 3; -2)$ appartient à \mathcal{P} ;
(b) $G(1; 3; 2)$ appartient à \mathcal{P} ;
(c) $G(1; 3; -1)$ appartient à \mathcal{P} .
5. (a) Le plan $\mathcal{Q}_1 : x + 2y - 3z + 1 = 0$ est orthogonal à \mathcal{P} ;
(b) le plan $\mathcal{Q}_2 : 4x - 5y - 2z + 3 = 0$ est orthogonal à \mathcal{P} ;
(c) le plan $\mathcal{Q}_3 : -3x + 2y - z - 1 = 0$ est orthogonal à \mathcal{P} .
6. (a) La distance du point $T(-1; -3; 2)$ au plan \mathcal{P} vaut $\sqrt{14}$;
(b) la distance du point $T(-1; -3; 2)$ au plan \mathcal{P} vaut 14;
(c) la distance du point $T(-1; -3; 2)$ au plan \mathcal{P} vaut $2\sqrt{3}$.

25.2 Second QCM



On munit l'espace d'un repère orthonormal.

Soient $S(1; -2; 0)$ et le plan \mathcal{P} d'équation cartésienne $x + y - 3z + 4 = 0$. Donner la réponse exacte parmi les quatre affirmations proposées :

1. Une représentation paramétrique de la droite \mathcal{D} passant par S et orthogonale à \mathcal{P} est :

(a) $\begin{cases} x = 1 + t \\ y = 1 - 2t \\ z = -3 \end{cases}$;

(b) $\begin{cases} x = 2 + t \\ y = -1 + t \\ z = 1 - 3t \end{cases}$;

(c) $\begin{cases} x = 1 + t \\ y = -2 - 2t \\ z = 3t \end{cases}$;

(d) $\begin{cases} x = 2 + t \\ y = -1 + t \\ z = -3 - 3t \end{cases}$.

2. Le point d'intersection de \mathcal{D} et du plan \mathcal{P} est :

(a) $H(-4; 0; 0)$;

(b) $H\left(\frac{6}{5}; -\frac{9}{5}; -\frac{3}{5}\right)$;

(c) $H\left(\frac{7}{9}; -\frac{2}{3}; -\frac{1}{3}\right)$;

(d) $H\left(\frac{8}{11}; -\frac{25}{11}; \frac{9}{11}\right)$;

3. La distance de S à \mathcal{P} vaut :

(a) $\frac{\sqrt{11}}{3}$;

(b) $\frac{3}{\sqrt{11}}$;

(c) $\frac{9}{\sqrt{11}}$;

(d) $\frac{9}{11}$.

4. L'intersection de la sphère \mathcal{S} de centre S et de rayon 3 avec \mathcal{P} est :

(a) le point $I(1; -5; 0)$;

(b) le cercle de centre H et de rayon $3\sqrt{\frac{10}{11}}$;

(c) le cercle de centre S et de rayon 2 ;

(d) le cercle de centre H et de rayon $3\frac{\sqrt{10}}{11}$.

DM 26. Dénombrement

26.1 Parties d'un ensemble

- ★
1. Montrer que le nombre de parties d'un ensemble à n éléments est 2^n .
On pourra faire une démonstration directe ou par récurrence.
 2. Sans utiliser la formule du binôme, prouver que $\sum_{p=0}^n \binom{n}{p} = 2^n$ en partitionnant l'ensemble des parties.

26.2 Problème des parties

★
★

Soit E un ensemble à n éléments, $n \geq 1$. On dresse la liste de toutes les parties de E , et chaque partie est recopiée sur un carton. On obtient donc 2^n cartons, que l'on suppose indiscernables et que l'on place dans une urne. On tire alors au hasard et sans remise deux cartons dans l'urne. On s'intéresse à la probabilité p que la réunion des deux parties tirées soit égale à E .

1. Résoudre ce problème à l'aide d'un arbre lorsque $n = 1$ puis $n = 2$.
2. Combien y a-t-il de tirages possibles dans le cas général ?
3. Soit A une partie de E à k éléments. Montrer que le nombre de parties B différentes de A telles que $A \cup B = E$ vaut 2^n si $k = n$ et 2^k sinon.
On pourra utiliser le complémentaire de A .
4. En déduire que le nombre de tirages favorables est

$$\sum_{k=0}^{n-1} \binom{n}{k} 2^k + 2^n - 1.$$

5. Utiliser la formule du binôme pour montrer que $p = \frac{3^n - 1}{2^n(2^n - 1)}$.
6. Quelle est la limite de p lorsque n tend vers l'infini ?

26.3 Dénombrement par partitionnement

- ★
★
1. Une urne contient n boules rouges et n boules vertes. Combien y a-t-il d'échantillons contenant k boules rouges et $n - k$ boules vertes ?
 2. En déduire que $\sum_{k=0}^n \binom{n}{k}^2 = \binom{2n}{n}$

26.4 Formule du binôme



Montrer la formule du binôme par récurrence.

On utilisera la propriété fondamentale des coefficients binômiaux.

26.5 Calculs de sommes binomiales



Soient f et g les fonctions définies sur \mathbb{R} par $f(x) = (1+x)^n$ et $g(x) = (1-x)^n$, où $n \geq 1$.

1. Développer $f(x)$ et $g(x)$ en utilisant la formule du binôme.
2. Calculer de deux manières, à partir des deux expressions obtenues précédemment (définitions et développements), $f'(x)$ et $g'(x)$.
3. En déduire les sommes

$$\sum_{k=1}^n k \binom{n}{k}$$

et

$$\sum_{k=1}^n (-1)^k k \binom{n}{k}.$$

26.6 Formule de Leibniz



Soient f et g deux fonctions dérivables, par exemple sur \mathbb{R} .

Donner une expression pour le développement de $(fg)^{(n)}$.

On commencera par conjecturer le résultat en prenant de petites valeurs de n , puis on démontrera la conjecture, par exemple par récurrence en s'inspirant de la preuve de la formule du binôme.

DM 27. Compléments de probabilités

27.1 Approximation par une loi de Poisson

★
★
★

On observe durant une longue période les accidents de scooter à un carrefour dangereux. On note S_n le total du nombre d'accidents, n étant un grand nombre inconnu. On admet que S_n suit une loi binomiale et que $E(S_n) = 10$.

1. Justifier l'égalité $P(S_n = k) = \binom{n}{k} \left(\frac{10}{n}\right)^k \left(1 - \frac{10}{n}\right)^{n-k}$ où $0 \leq k \leq n$.
2. (a) Montrer que $\lim_{n \rightarrow +\infty} P(S_n = 0) = e^{-10}$.
(b) Montrer que $P(S_n = k + 1) = P(S_n = k) \frac{n - k}{n - 10} \frac{10}{k + 1}$ où $0 \leq k \leq n - 1$.
(c) Montrer par récurrence que $\lim_{n \rightarrow +\infty} P(S_n = k) = e^{-10} \frac{10^k}{k!}$ où $0 \leq k \leq n$.
3. On suppose que n est suffisamment grand pour que $e^{-10} \frac{10^k}{k!}$ soit une bonne approximation de $P(S_n = k)$ (c'est l'approximation d'une loi binomiale par une loi de Poisson). Utiliser cette approximation pour calculer la probabilité qu'il y ait au moins 3 accidents de scooter.

27.2 Simulation de la loi exponentielle

★
★

On dispose d'un générateur de nombres pseudo-aléatoires entre 0 et 1. On souhaite simuler les valeurs d'une variable aléatoire $X \sim \mathcal{E}(\lambda)$.

1. Tracer schématiquement sa fonction de répartition F .
2. Choisir au hasard un y dans $]0; 1[$ puis placer sur le schéma son antécédent x par F .
3. Exprimer par le calcul x en fonction de y .
4. Soit $U \sim \mathcal{U}(]0; 1[)$. Montrer que $X = -\frac{1}{\lambda} \ln(1 - U)$ suit la loi exponentielle de paramètre λ , en déterminant sa fonction de répartition.
Pourquoi en est-il de même pour $\tilde{X} = -\frac{1}{\lambda} \ln(U)$?
C'est la méthode de la pseudo-inverse (de la fonction de répartition).

27.3 Fonction gamma

★

Lorsque $x \geq 1$, on définit la fonction gamma par $\Gamma(x) = \int_0^{+\infty} t^{x-1} e^{-t} dt$.

1. Montrer que $\Gamma(x + 1) = x\Gamma(x)$ et que $\Gamma(1) = 1$.
2. En déduire que $n! = \Gamma(n + 1)$.
Si l'on définit ainsi la factorielle alors on trouve naturellement $0! = 1$.

27.4 Loi faible des grands nombres

★
★
★

Soit X une variable aléatoire discrète d'espérance μ et de variance σ^2 .

1. Montrer que $\sigma^2 \geq \sum \varepsilon^2 P_X(x_i)$, la somme étant prise sur toutes les valeurs x_i de X vérifiant $|x_i - E(X)| \geq \varepsilon$.
2. En déduire que $P(|X - E(X)| \geq \varepsilon) \leq \frac{\sigma^2}{\varepsilon^2}$ (*théorème de Bienaymé-Tchebychev*).
3. *Application.* Soient X_1, \dots, X_n des variables aléatoires indépendantes et de même loi, de variance σ^2 et d'espérance μ . On note $S_n = X_1 + \dots + X_n$. Montrer que la limite de $P\left(\left|\frac{S_n}{n} - \mu\right| \geq \varepsilon\right)$ lorsque n tend vers $+\infty$ vaut 0 (*loi faible des grands nombres* : la moyenne de valeurs aléatoires tend en probabilité vers la moyenne sous-jacente).
4. *Application.* Montrer que lorsqu'on lance une pièce de monnaie, la fréquence de « pile » tend (au sens *faible*) vers $\frac{1}{2}$.

DM 28. Autour de la loi normale

28.1 Méthode de Monte-Carlo

28.2 Mélange de gaz

28.3 Test de normalité

Partie IV

Devoirs à la maison – Spécialité

DM 1. Méthode de Fermat

La factorisation des entiers est un domaine de recherche très actif et d'une *grande importance*. En effet, la difficulté (i.e. le temps nécessaire) à factoriser un entier est à la base de certains systèmes modernes de *cryptage*, tel le RSA, utilisé abondamment sur internet par exemple.

On présente ici une méthode élémentaire due à Pierre de Fermat (mathématicien français, 1601-1665), qui est à la base de résultats beaucoup plus évolués qui forment des algorithmes parmi les plus performants actuellement (famille des *cribles quadratiques*).

Notre but est donc de comprendre cette méthode en factorisant un entier naturel n . Attention cependant, on ne décrit pas ici une méthode pour déterminer tous les facteurs premiers de n , mais juste pour écrire n comme un produit non trivial de deux entiers.

1.1 Introduction



- (a) Trouver *sans calculatrice* deux entiers naturels supérieurs à 1, l'un pair et l'autre impair, dont le produit fasse 10672.
(b) Soit n un entier naturel non nul. Décrire une procédure qui permet de décomposer n en produit pq , où p est pair et q impair.

Dans toute la suite, on suppose donc que n est un entier naturel impair.

- Supposons maintenant que n soit *composé*, i.e. qu'il s'écrive $n = uv$, où u et v sont des entiers naturels.
 - Que peut-on dire de la parité de u et de celle de v ?
 - Posons $a = \frac{u+v}{2}$ et $b = \frac{|u-v|}{2}$. Montrer que a et b sont des entiers.
 - Montrer que $n = a^2 - b^2$.
Ainsi, tout entier naturel impair peut s'écrire comme la différence du carré de deux entiers naturels.

- On donne $8051 = 90^2 - 7^2$. Factoriser sans calculatrice le nombre 8051.
 - Revenons au cas général. Supposons maintenant que nous ne connaissons pas encore la factorisation éventuelle de n , mais que nous avons trouvé ces deux entiers a et b tels que $n = a^2 - b^2$.

Factoriser n .

Ainsi, si l'on trouve deux entiers a et b tels que $a^2 = b^2 + n$, alors n se factorise.

1.2 Algorithme



- Donnons-nous un entier impair, disons $n = 1081$. Prenons sa racine carrée (32,87...) puis l'entier juste au-dessus de ce nombre (33 donc). Élevons-le au carré (1089) puis

soustrayons-lui n (ce qui donne 8). Le nombre 8 n'est pas un carré, on recommence. On prend le nombre 34, pour lequel on obtient $34^2 - n = 75$ qui n'est toujours pas un carré. On prend 35, et on arrive cette fois à $35^2 - n = 144 = 12^2$. C'est gagné !

- (a) Factoriser 1081 grâce à l'égalité précédente.
- (b) Factoriser par la même méthode les entiers 4959 puis 3479605.
- (c) Revenons au cas général.

Montrer que, si $n = uv$ (cf question 2), alors $a > \sqrt{uv}$. Pourquoi, en partant de $\lceil \sqrt{n} \rceil$ comme décrit sur l'exemple $n = 1081$, sommes-nous sûrs de ne pas rater le nombre a ?

- (d) Écrire un algorithme qui prend en entrée un entier impair n et qui retourne une factorisation de n par la méthode ci-dessus.
- (e) Écrire le programme correspondant sur calculatrice.
- (f) Tester ce programme et rédiger la procédure de test réalisée.

DM 2. Polynômes à coefficients entiers

Dans ce problème, on va déterminer l'existence et la valeur des racines rationnelles d'un polynôme à coefficients entiers.

2.1 Racines rationnelles



Soit P un polynôme défini pour tout réel x par $P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ où a_0, \dots, a_n sont des entiers.

1. Soient p un entier relatif et q un entier naturel non nul, tels que la fraction $\frac{p}{q}$ soit irréductible. Supposons que cette fraction soit racine du polynôme P .
 - (a) Si d est un diviseur commun de p et de q , que peut-on dire de sa valeur ?
 - (b) Exprimer l'équation $P\left(\frac{p}{q}\right) = 0$ en utilisant uniquement des entiers.
 - (c) Exprimer $-a_0 q^n$ à partir des autres données, en utilisant la question précédente. Montrer que p divise a_0 .
 - (d) Montrer de la même manière que q divise a_n .
2. On suppose maintenant, ce qui est courant en pratique, que le coefficient dominant a_n vaut 1.
Que peut-on alors conclure quant à la nature des racines de P ?

2.2 Applications



1.
 - (a) Montrer, en considérant le polynôme $P(x) = x^2 - 2$, que le nombre $\sqrt{2}$ est irrationnel.
 - (b) Quelle est la nature du nombre \sqrt{k} , où k est un entier supérieur ou égal à 2 ?
2. Trouver les racines rationnelles, puis résoudre les équations :
 - (a) $x^3 + 4x^2 + 9x + 6 = 0$;
 - (b) $x^3 - 9x^2 + 26x - 24 = 0$;
 - (c) $\frac{3}{2}x^3 + x^2 + x - \frac{1}{2} = 0$;
 - (d) $x^3 - x^2 - \frac{x}{4} + \frac{1}{4} = 0$;
 - (e) $2x^5 - 11x^4 + 14x^3 - 2x^2 + 12x + 9 = 0$.

DM 3. Nombres de Mersenne

Pour q entier naturel, $M_q = 2^q - 1$ est le q -ième nombre de Mersenne.

On supposera en général dans la suite $q \geq 3$ par commodité.

On rappelle les identités remarquables jumelles $a^k - 1 = (a - 1)(a^{k-1} + a^{k-2} + \dots + a + 1)$ et $a^k + 1 = (a + 1)(a^{k-1} - a^{k-2} + \dots - a + 1)$, k étant impair pour la deuxième.

3.1 Racine carrée modulaire de 2

★

Si q est impair, montrer que $x = 2^{\frac{q+1}{2}}$ vérifie $x^2 \equiv 2 \pmod{M_q}$.

3.2 Factorisation de M_q

★

★

1. Écrire un programme qui renvoie la liste des entiers $q \leq 100$ tels que M_q soit premier. Que remarque-t-on ?
2. Si q est composé, montrer que M_q se factorise.
3. Si M_q est premier, que peut-on en déduire sur q ?

3.3 Factorisation de M_{11}

★

★

1. Peut-on a priori affirmer que M_{11} est composé ?
2. Donner une racine carrée de 2 modulo M_{11} .
3. Montrer que $2(2^6 - 8)^2 \equiv (2^6 + 1)^2 \pmod{M_{11}}$.
4. En déduire que $2^{12}(2^6 - 8)^2 \equiv (2^6 + 1)^2 \pmod{M_{11}}$.
5. Montrer que M_{11} divise $[2^6(2^6 - 8) - (2^6 + 1)][2^6(2^6 - 8) + (2^6 + 1)]$.
6. Calculer concrètement M_{11} et $2^6(2^6 - 8) + (2^6 + 1)$ puis déterminer leur pgcd.
7. Factoriser M_{11} .
8. Si q premier, est-on assuré que M_q le soit ?

3.4 Pgcd de deux nombres de Mersenne

- ★
 - ★
 - ★
1. À l'aide de l'algorithme d'Euclide, calculer le pgcd de M_{12} et M_8 puis celui de M_{14} et M_{10} . Quelle conjecture sur le pgcd peut-on émettre ?
 2. Soient a et b deux entiers tels que $0 < b \leq a$. Soit r le reste de la division euclidienne de a par b . Montrer que M_r est le reste de la division euclidienne de M_a par M_b .
 3. Soit d le pgcd de a et b . En appliquant l'algorithme d'Euclide, montrer que le pgcd de M_a et M_b est M_d .
 4. Si a et b sont premiers entre eux, que peut-on affirmer sur M_a et M_b ?

DM 4. Nombres de Fermat

Pour q entier naturel $F_q = 2^{2^q} + 1$ le q -ième *nombre de Fermat*.

On rappelle les identités remarquables jumelles $a^k - 1 = (a - 1)(a^{k-1} + a^{k-2} + \dots + a + 1)$ et $a^k + 1 = (a + 1)(a^{k-1} - a^{k-2} + \dots - a + 1)$, k étant impair pour la deuxième.

4.1 Racine carrée modulaire de 2

★

Vérifier que $2^{2^q} \equiv -1 \pmod{F_q}$ puis montrer que $x = 2^{3 \cdot 2^{q-2}} - 2^{2^{q-2}}$ vérifie $x^2 \equiv 2 \pmod{F_q}$.

4.2 Origine des nombres de Fermat

★

★

1. Écrire un programme qui renvoie la liste des entiers $k \leq 100$ tels que $2^k + 1$ soit premier. Que remarque-t-on ?
2. Supposons donc maintenant que $2^k + 1$ soit premier. On pose $k = a \cdot 2^b$ où a est impair (b représente donc le nombre de "2" dans la décomposition de k en facteurs premiers) et $c = 2^{2^b}$. Vérifier que $2^k + 1 = c^a + 1$.
3. Montrer que $c^a + 1 = (c + 1)(c^{a-1} - c^{a-2} + \dots \pm a \mp 1)$.
4. En déduire que $c + 1 = 2^k + 1$ puis que $k = 2^b$.
5. À quelle famille appartiennent les nombres de la forme $2^k + 1$ qui sont premiers ?

4.3 Primalité des nombres de Fermat

★

1. Vérifier que F_1, F_2, F_3, F_4 sont premiers.
2. Montrer par réductions modulaires successives que $2^{32} \equiv -1 \pmod{641}$. Le nombre F_5 est-il premier ?

4.4 Pgcd de deux nombres de Fermat

★

★

1. Vérifier que $F_q = (F_{q-1} - 1)^2 + 1$ et en déduire que $F_q - 2 = F_{q-1}(F_{q-1} - 2)$.
2. Montrer par récurrence que $F_q - 2 = \prod_{k=0}^{q-1} F_k$.
3. Soit $q' < q$. Montrer qu'un diviseur commun de F_q et $F_{q'}$ divise 2.
4. En déduire que deux nombres de Fermat distincts sont premiers entre eux.

DM 5. Formes de nombres premiers

5.1 La forme $4n + 1$

- ★ Soit a un entier naturel *pair* non nul.
1. Soit p un nombre premier divisant $a^2 + 1$.
 - (a) Quelle est la parité de $a^2 + 1$?
 - (b) En déduire que p est soit de la forme $4n + 1$, soit de la forme $4n + 3$.
 - (c) Montrer que $a^4 \equiv 1 \pmod{p}$.
 - (d) Montrer, en utilisant le petit théorème de Fermat, que $a^{p-1} \equiv 1 \pmod{p}$.
 - (e) Supposons que p s'écrive sous forme $4n + 3$. En utilisant la question (c), montrer que $a^{p-1} \equiv -1 \pmod{p}$.
 - (f) Déduire des questions précédentes que $p = 2$.
 - (g) Le nombre p peut-il s'écrire sous la forme $4n + 3$?
 2. Soit $N \geq 2$ un entier, et soit $a = N!$.
 - (a) Pourquoi existe-t-il un nombre premier p divisant $a^2 + 1$?
 - (b) Montrer que p est de la forme $4n + 1$.
 - (c) Montrer que p ne divise pas a , et en déduire $p > N$.
 - (d) Montrer qu'il existe une infinité de nombres premiers de la forme $4n + 1$.

5.2 La forme $6n + 1$

- ★ Soit x un entier naturel non nul, multiple de 6.
Soit p un nombre premier divisant $x^2 + x + 1$.
1. En travaillant modulo 6, montrer que p est différent de 2 et 3, et s'écrit sous la forme $6n + 1$ ou $6n + 5$ avec $n \geq 1$.
 2. Montrer que $x^3 \equiv 1 \pmod{p}$, puis que $x^{6n} \equiv 1 \pmod{p}$ pour tout entier naturel n .
On rappelle que $x^3 - 1 = (x - 1)(x^2 + x + 1)$...
 3. On suppose que $p = 6n + 5$. Montrer que $x \equiv 1 \pmod{p}$. Que vaut alors p ?
 4. Déduire de ce qui précède que p est de la forme $6n + 1$.
 5. Soit $N \geq 3$ un entier. On pose $x = N!$. Prouver que $p > N$.
 6. Montrer qu'il existe une infinité de nombres premiers de la forme $6n + 1$.

DM 6. Ordre

6.1 Ordre modulo p

- ★ Soit p un nombre premier et soit a un entier naturel non nul premier avec p .
- ★
 1. Montrer que l'ensemble des entiers $k \geq 1$ tels que $a^k \equiv 1 \pmod{p}$ n'est pas vide.
 2. On désigne alors par s le plus petit élément de cet ensemble.
Soit $k \geq 1$ un entier tel que $a^k \equiv 1 \pmod{p}$.
 - (a) Montrer que le reste r de la division euclidienne de k par s vérifie $a^r \equiv 1 \pmod{p}$.
 - (b) En déduire que $r = 0$ puis que s divise k .
 3. Montrer alors que s divise $p - 1$.

Le nombre s est l'ordre de a modulo p .

6.2 Théorème de Wilson

- ★
 1. Soit $p \geq 5$ un nombre premier et soit $A = \{2, \dots, p-2\}$. Montrer que, pour tout x dans A , $x^2 - 1$ n'est pas divisible par p .
 2.
 - (a) Soit x dans A ; prouver qu'il existe un entier u tel que $xu \equiv 1 \pmod{p}$.
 - (b) En déduire l'existence d'un unique entier r de A , distinct de x , tel que $xr \equiv 1 \pmod{p}$.
 - (c) Etablir alors que $2 \times \dots \times (p-2) \equiv 1 \pmod{p}$, puis que $(p-1)! \equiv -1 \pmod{p}$.
 3. Ce résultat demeure-t-il vérifié lorsque $p = 2$ et $p = 3$?
 4. Réciproquement, soit $p \geq 2$ tel que $(p-1)! \equiv -1 \pmod{p}$.
Montrer, en utilisant Bézout, que p est premier.
 5. En déduire le théorème de Wilson : un nombre p est premier ssi $(p-1)! + 1 \equiv 0 \pmod{p}$.
 6. Ce critère de primalité est-il efficace du point de vue algorithmique?
- ★

DM 7. Nombres de Carmichael et critère de Korselt

7.1 Introduction

★ **Nombres pseudo-premiers de Fermat** Un entier strictement positif n tel que $a^n \equiv a \pmod{n}$ est un *nombre pseudo-premier de Fermat* en base a .

Problème On sait, par le petit théorème de Fermat, que pour tout nombre premier p et tout entier a , $a^p \equiv a \pmod{p}$. La réciproque de ce résultat, appelée *test de Fermat*, est fausse. Cependant, en cherchant une méthode simple et rapide pour distinguer les nombres premiers des nombres composés, on pourrait penser à combiner des tests de Fermat pour *différentes* bases a .

Exercice Montrer que 341 est un pseudo-premier en base 2 mais non en base 3. Réciproquement, prouver que 91 est un pseudo-premier en base 3 mais non en base 2.

Introduction aux nombres de Carmichael Peut-être n'existe-t-il pas de nombres composés qui sont simultanément pseudo-premiers en bases 2 et 3? Malheureusement, $561 = 3 \cdot 11 \cdot 17$ n'est pas seulement un pseudo-premier de Fermat en bases 2 et 3, mais est également un pseudo-premier dans *toute* base a .

De tels nombres furent découverts par Carmichael en 1910.

Nombres de Carmichael Un entier composé n pour lequel $a^n \equiv a \pmod{n}$ pour tout entier a est *nombre de Carmichael*.

Reconnaître les nombres de Carmichael Il est facile de reconnaître un nombre de Carmichael à partir de sa décomposition en facteurs premiers. Ce résultat est le *critère de Korselt*, que nous allons démontrer.

Nombres sans facteur carré Un entier n est *sans facteur carré* si pour tout premier p divisant n , p^2 ne divise pas n .

Critère de Korselt Un entier n est un nombre de Carmichael ssi n est strictement positif, composé, sans facteur carré, et tel que pour tout premier p divisant n , $p - 1$ divise $n - 1$.

7.2 Preuve du théorème de Korselt

- ★
 - ★
 - ★
1. Premièrement, supposons que n est un nombre de Carmichael.
 - (a) Vérifier que n est composé.
 - (b) Soit p un facteur premier de n . En utilisant $p^n \equiv p \pmod{n}$, montrer que p^2 ne divise pas n .
 - (c) On admet qu'il existe a une *racine primitive* modulo p , i.e. $2 \leq a < p$, $\text{pgcd}(a, p) = 1$ et l'ordre de a modulo p vaut $p - 1$. Montrer que $a^{n-1} \equiv 1 \pmod{p}$ et que $p - 1$ divise $n - 1$.
 2. Réciproquement, supposons que n est composé, sans facteur carré, et que pour chaque premier p divisant n , $p - 1$ divise $n - 1$.
 - (a) Montrer qu'il suffit de prouver que $a^n \equiv a \pmod{p}$ pour tout premier p divisant n .
 - (b) Supposons que $p \mid n$ et que a est un entier.
 - Si a n'est pas divisible par p , montrer que $a^{p-1} \equiv 1 \pmod{p}$, et $a^{n-1} \equiv 1 \pmod{p}$ aussi. Ainsi, $a^n \equiv a \pmod{p}$.
 - Si a est divisible par p , montrer que $a^n \equiv a \pmod{p}$.

DM 8. Coût de l'algorithme d'Euclide

★ Le but de l'étude est de contrôler le nombre de divisions successives nécessaires à l'aboutissement de l'algorithme d'Euclide.

★ On note l'algorithme d'Euclide appliqué à n et k , avec $k < n$:

$$\begin{aligned}n &= q_0 k + r_0 \\k &= q_1 r_0 + r_1 \\r_0 &= q_2 r_1 + r_2 \\&\vdots \\r_i &= q_{i+2} r_{i+1} + r_{i+2} \\&\vdots \\r_{m-3} &= q_{m-1} r_{m-2} + r_{m-1} \\r_{m-2} &= q_m r_{m-1} + r_m\end{aligned}$$

où $r_m = 0$ et donc $n \wedge k = r_{m-1}$.

1. Montrer que l'algorithme est le moins performant lorsque tous les q_i valent 1 et $n \wedge k = 1$.
2. En déduire r_i en fonction de r_{i+1} et r_{i+2} , et vérifier que $r_{m-1} = 1$.
3. On rappelle que la suite de Fibonacci est définie par $F_0 = 0$, $F_1 = 1$ et $F_n = F_{n-1} + F_{n-2}$.
Montrer que n est le nombre de Fibonacci F_{m+2} .
4. (-> théorème de Lamé, à compléter)

DM 9. Fonction indicatrice d'Euler



On choisit au hasard uniforme l'un des nombres $1, 2, \dots, n$.

Soit p un entier vérifiant $1 \leq p \leq n$. Soit $A_p = \ll \text{le nombre choisi est divisible par } p \gg$.

1. Modéliser ce problème, i.e. donner l'univers Ω et la probabilité P .
2. Lorsque p divise n , calculer $P(A_p)$.
3. Si p_1, \dots, p_k sont des diviseurs premiers distincts de n , montrer que les événements A_{p_1}, \dots, A_{p_k} sont indépendants (i.e. la propriété du produit est valable pour n'importe quelle intersection d'événements A_j).
4. La *fonction indicatrice d'Euler* est la fonction ϕ définie sur \mathbb{N} qui donne le nombre $\phi(n)$ d'entiers non nuls inférieurs à n et premiers avec n .
Calculer $\phi(1), \dots, \phi(10)$.

5. Soit B_n l'ensemble des entiers inférieurs ou égaux à n et premiers avec n .

(a) Montrer que $B_n = \bigcap_{i=1}^k \overline{A_{p_i}}$.

(b) Montrer que $P\left(\bigcap_{i=1}^k \overline{A_{p_i}}\right) = \prod_{i=1}^k P(\overline{A_{p_i}})$.

(c) En déduire que $P(B_n) = \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right)$.

6. Vérifier que $P(B_n) = \frac{\phi(n)}{n}$ et en déduire :

$$\phi(n) = n \prod_{\substack{p \text{ premier} \\ p|n}} \left(1 - \frac{1}{p}\right)$$